WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE, State Bar No. 178960
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C01-1640 SBA Consolidated with C02-0647 SBA **MICROSOFT'S PRELIMINARY INVALIDITY CONTENTIONS REGARDING U.S. PATENTS 6,253,193 & 6,185,683 PURSUANT TO PLR 3-3, 3-4**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counterclaim-Defendant.	The Honorable Saundra B. Armstrong

InterTrust and its agents have engaged in a long pattern of misconduct that extends to and includes false and unsupported allegations of patent infringement. By way of example, the following information and attached charts illustrate that InterTrust has made invalid assertions of patent claim infringement under 35 U.S.C. §§ 102, 103 and 112 (limited to indefiniteness, non-enablement, and written description). Additional grounds for invalidity and unenforceability lie outside the scope of PLR 3-3 and are expressly reserved. Microsoft further reserves the unrestricted right to assert its defenses (and seek declaratory judgments) that the claims asserted by InterTrust are not infringed.

Microsoft has stated and preserves its objections and arguments as set forth in its motions on file and case management statements. Microsoft further notes and incorporates by reference its objections to InterTrust's improper attempts to modify its PLR 3-1 Statements without consent or leave of Court. Without limitation, Microsoft objects to InterTrust's refusal to provide a complete PLR 3-1 Statement for any of the InterTrust asserted patents, or to provide relevant information sought in discovery, including the identity of the alleged inventors of specific claims; conception or actual reduction to practice dates for specific claims; whether to its knowledge there has ever been any alleged embodiment(s) of asserted claims; and what if any specification support is alleged, including from any of the applications from which InterTrust claims priority. For example, InterTrust has failed to provide discovery regarding reduction to practice, including as set forth in Microsoft's motion to compel and the Court's rulings thereon. For another example, InterTrust has alleged that specific claims are entitled to rely on one or more earlier applications for priority, but has refused to state how. Microsoft expressly reserves the right to rely upon InterTrust's own activities, alone and in connection with others, as prior art, should InterTrust fully comply with relevant discovery. Microsoft further reserves the right to supplement this statement or otherwise further respond if InterTrust modifies its PLR 3-1 allegations (including but not limited to providing proper initial PLR 3-1 Statements), whether through motion or consent, or if InterTrust contends (or the Court rules) that any earlier or later priority date(s) may apply.

PLR 3-3(a, b)

This Statement responds to InterTrust's initial PLR 3-1 Statement regarding U.S. Patents 6,253,193 and 6,185,683 served on or about October 29, 2001. The identities of prior art references that anticipate claims as asserted in InterTrust's PLR 3-1 Statement or render them

obvious are set forth below and in the attached PLR 3-3(c) charts. Please refer to the columns in the charts for further description of the references identified in abbreviated form below.

Asserted Claims	**References That Anticipate and/or Render Obvious**
'683 - 2, 28-29	Stefik, CUPID, CNI/IMA 94, Choudhury/Maxemchuk, Tygar/Yee, Neuman, Davies & Price, ATMs, Chaum, Telescript, NT, Bell-Lapadula, CUPID, Blaze, "secure" OODBs,Kerberos, Cox/Mori, Griswold, Cryptolopes, iOpener, iPower, Lampson
'193 - 1-4, 11, 15, 19	Stefik, Choudhury/Maxemchuk, Blaze, CNI/IMA 94, Hellman, CUPID, Chaum, Neuman

See also the cited art in the manner applied by the Examiners.

Each prior art reference identified herein and in the attached charts anticipates one or more asserted claims or renders them obvious. People having knowledge of this information prior to relevant priority dates include the authors/creators and recipients/users of each reference.

Entities making/receiving offers or information regarding products referenced herein include the following:

Item	**Date**	**exemplary entities making offer and/or information known**
NT, OLE, COM	1993 and continuing thru at least 2/12/95 and 2/24/97	Microsoft Corp.
Kerberos	before 1994 and continuing thru at least 2/12/95 and 2/24/97	MIT; B. Clifford Neuman
Strongbox, Dyad, Mach	before 1994 and continuing thru at least 1995	Carnegie Mellon Univ.; Doug Tygar; Bennet Yee, Rick Rashid
Stefik	at least by 1994 and continuing thru at least 2/12/95 and 2/24/97	Xerox; ContentGuard
CUPID	at least by 2/94 and continuing thru at least 2/12/95 and 2/24/97	See '683 chart
PolicyMaker	by 1996	AT&T
PersonaLink	at least prior to 2/12/95	AT&T
Telescript	at least by 1994	General Magic, AT&T, RSA
PGP	at least by 2/94 and continuing	Phil Zimmerman

1

	thru at least 2/12/95 and 2/24/97	
RSA software	at least before 2/12/95 and 2/24/97	RSA
iPower, iOpener	before 2/12/95	National Semiconductor
"secure" OODB systems (e.g., Orion, Itasca, Thor)	at least by 2/13/94 and continuing thru at least 2/12/95 and 2/24/97	MCC, Itasca, MIT (see '683 chart); IBEX
Cryptolope & InfoMarket	Before 2/12/95 and 2/24/97	IBM

From InterTrust's current document production, it appears that its employees' and consultants' activities, including offers for sale, public uses, derivations, and "inventions" (in the sense of Section 102(g)), and disclosures to Willis Ware, Drew Dean, and others not under any duty of confidentiality, constituted or created material and perhaps anticipatory prior art to many of the asserted claims, that was not cited to the Patent Office. Microsoft reserves the right to supplement this disclosure after Microsoft has had an opportunity to investigate this possible prior art in discovery.

Suggestions to combine & motivations to combine

Among the combinations obvious under § 103 are those set forth in each § 102 prior art reference cited herein, including D. Kahn, The Codebreakers (Macmillan 1967); L.D. Smith, Cryptography – the science of secret writing (Dover 1943, 1971); Bruce J. Walker and Ian F. Blake, Computer Security and Protection Structures (Dowden Hutchinson & Ross, Inc. 1977); D. Hsiao et al., Computer Security (Academic Press 1979); A. Konheim, Cryptography: A Primer (Wiley 1981); D. Denning, Cryptography and Data Security (Addison-Wesley 1982); Meyer, C.H., and Matyas, S.M., Cryptography - A New Dimension in Computer Data Security (Wiley 1982); Wood, Unix System Security (Hayden 1985); Elliott Irving Organick, The Multics System (MIT 5th ed. 1985); C.J. Date, An Introduction to Database Systems, 4th ed. (Addison-Wesley 1986); J. Cooper, Computers & Communications (McGraw Hill 1989); S. Muftic, Security Mechanisms for Computer Networks (Ellis Horwood 1989); Davies & Price, Security For Computer Networks (Wiley 1989); W. LaLonde and J. Pugh, Inside Smalltalk (Prentice Hall 1990); Computer Security (Time Life 1990); D. Russell et al., Computer Security Basics (O'Reilly 1991); S. Garfinkel, Practical Unix Security (O'Reilly 1991); CMU Computer Science: A 25th Anniversary Commemorative, R. Rashid, ed. (ACM Press 1991); D. Curry, Unix System

Security (Addison-Wesley 1992); Custer, Inside NT (Microsoft Press 1993); B. Schneier, Applied Cryptography (Wiley 1994) (also 2d ed. 1996); D. Dougherty, The Mosaic Handbook (O'Reilly 1994); Castano, Database Security (Addison-Wesley 1994); F. Cohen, Protection and Security on the Information Highway (Wiley 1995); A. Tanenbaum, Operating Systems, Design and Implementation (Prentice Hall 1987), Computer Networks, 2d ed. (Prentice Hall 1988), Modern Operating Systems (Prentice Hall 1992), and Distributed Operating Systems (Prentice Hall 1995); the work of Martin S. Olivier et al. cited in the attached '683 chart; the work of Morris Sloman, Jonathan Moffet, David Chaum, B. Clifford Neuman and Butler Lampson (see www.doc.ic.ac.uk/~mss/MSSPubs.html; www-users.cs.york.ac.uk/~jdm/jdmpubs.htm ; www.chaum.com/articles/list_of_articles.htm; http://www.isi.edu/people/bcn/publications.html; and research.microsoft.com/lampson/Publications.html); any single conference, meeting or proceedings, such as the January 1994 RSA Data Security Conference,[2] the April 1993 conference at Harvard University described in the deposition of Richard J. Linn, or Proceedings, Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project, vol. 1 no. 1 (Jan. 1994) ("CNI/IMA 94"). Additional obvious combinations include the combinations indicated in the asserted patents' file histories, related RFCs, work on a common project or product, and the combinations of any given author or named inventor's cumulative prior art work. For example, by "Stefik" this document refers to the referenced patents, acts and publications attributed in whole or part to Mark Stefik, taken individually or together. These make obvious, for example, that using methods in additive, iterative or other combinations could enhance overall "security," as would variation in individual steps or methods, such as encrypting, signing, or building files, using objects, and/or distributing in such a manner as to help do or protect things of value against unauthorized access, threats, or adverse effects. Adding or subtracting rights, or adding or repeating steps or functions (such as adding Kerberos to access control lists or capabilities, or watermarking binaries before and/or after encrypting any part of them), were simple variations of this. (See, e.g., Davies, Denning, Hellman, Neuman, Chaum, Linn, Blaze, Lampson, Tygar/Yee, Stefik, Choudhury/Maxemchuk, Moffett, Curry, Garfinkel/Spafford, Muftic, Carroll, Hsiao et al.). These further make obvious that one can automate any manual step

[2] See, e.g., Walker, Notes from RSA Data Security Conference, www.eff.org/Privacy/Crypto/Crypto_misc/rsa_conf.summary (Jan. 18, 1994); www.ddj.com/documents/s=1005/ddj9454d/9454d.htm, (Dr. Dobbs Journal).

in the exchange of encrypted information, or vice versa. For example, one or more steps of a communication or transfer could be "out of band".

The motivation for seeking "security," privacy, and integrity was widely recognized in the United States and elsewhere prior to February 13, 1994, and extends to any information or item of perceived value, including books, music, computer systems, and computer programs, as set forth in, e.g., Hellman, Stefik, Chaum, Choudhury, Date, Castano, Custer, Olivier, Russell, Muftic, Denning and/or Davies.[3] Additional motivations include the desire to meet or exceed any applicable laws or industry or government standards, such as the Orange Book, Computer Fraud and Abuse Act of 1986, Computer Security Act of 1989 PL100-35, High Performance Computing Act (HPCA) of 1991 (P.L. 102-194), and Title 17 U.S.C. § 101 et seq. (including, for example, § 1002). Industry standards include those for communication, such as X.509, TCP/IP, WWW, and WAIS, and those for encryption or transmission of encrypted information, e.g., DES, Triple DES, RSA, SSL, S/MIME, SHTTP, HTTPS, MD5, and PEM. Additional obviousness teachings to combine with such items or information include "security" levels, permissions, certificates, tickets, "secure" processors, "secure" storage, "smart" cards (including smart cards able to store data and perform computations such as encryption/decryption), tamper resistance techniques for hardware and software, physical "security," trusted time, authentication and authorization in trusted distributed systems, enabling software or features thereof to run only on particular machines, and treating binary information/data at varied levels of granularity. It was further obvious to combine any of these "security" features with any of the following software (or features thereof) and/or any of the following hardware (or features thereof) to provide any element or perform any step shown in the charts below:

> software: file and operating systems such as NT, NFS, Andrew, Netware, Mach, DT Mach, Multics, Unix, and in the Blaze and Tanenbaum and other references cited above; secure kernels; protocols, codes and systems such as WWW, SSL, SGML, hypertext, Oak, Telescript, OOP and other programming technologies or frameworks (e.g. Smalltalk, COM, OLE, Bento, Open Doc)[4]; object-oriented databases; watermarking; obfuscation (see, e.g., Choudhury at 15); swIPe; SNMP; auditing; on-line transaction and

[3] Regarding digital music, see also, e.g., J. Ratcliff, "Examining PC Audio," Dr. Dobb's Journal (March 1993).

[4] For example, it was obvious to use the prior art OOP technologies or frameworks to implement the systems described in e.g. Fischer, Linn, Stefik, Choudhury, Telescript, and object-oriented databases.

subscription-based services and billing; electronic payment; on-line banking, entertainment and commercial and interactive commerce; encryption and authentication (including e.g., "something you are, something you know, something you have"); hardware: physical security tools and devices; physically secure locations, physically "secure" products such as tamper resistant computers or other devices, "secure" processors, "secure" memory, "smart" cards, set-top boxes, portable devices, "secure" communication facilities.

See Stefik, CNI/IMA 94, Chaum, Tygar/Yee, Choudhury/Maxemchuk, Stefik, Denning, Davies, Moffett, Curry, Garfinkel/Spafford, Muftic, Carroll, Hsiao et al. and the other references cited above.

Each of these suggestions and motivations to combine apply to each of the references set forth in the attached charts.

PLR 3-3(c)

The attached charts identify, for each item of prior art, elements within the scope of InterTrust's October 29, 2001 PLR 3-1 allegations for the '683 and '193 patents. The structure, act or material for any such element if so construed is set forth in the references identified in the attached charts.[5]

PLR 3-3(d)

Each asserted claim is invalid as indefinite, for lack of enablement, and for lack of the written description required by statute. The present basis in each case is each applicable patent specification relied upon by InterTrust for the description required by paragraphs one and two of Section 112, and the prosecution histories of those applications and related applications as provided by law. Further basis may include, by way of example, any extrinsic evidence relevant to the construction of claim terms; InterTrust's own professed ignorance whether simple acts like playing music from a compact disc do not infringe asserted claims; and its difficulty, delay and/or inability to identify conception dates or actual reductions to practice of asserted claims.

[5] InterTrust has not identified any claim elements allegedly subject to § 112 ¶ 6 under PLR 3. Should InterTrust do so (and reserving any objection thereto), Microsoft reserves the right to respond to that issue.

"Indefiniteness" of the Asserted InterTrust Patent Claims[6]

In prosecuting, marketing, and enforcing the asserted InterTrust Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents. For example, InterTrust has mechanically buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the claims, and has buried the Examiners with hundreds or thousands of pages of redundant, verbose, unclear text, effectively precluding a real comparison of the alleged "invention" versus the prior art, and accused non-infringing products of infringement. One result of InterTrust's approach is that the asserted patent claims are indefinite in myriad ways.

The asserted "claims" are unclear in scope and not nearly as precise as the subject matter allows. This indefiniteness arises from many causes, including:

- by use of terms that lacked any ordinary meaning in the art and are undefined in the specification;
- by use of terms that are used in the specification in a manner inconsistent with their ordinary meaning, but are not specifically defined in the specification;
- by a Section 112, ¶ 6 "means (or step) plus function" element having no specific structure in the application's written description clearly linked to that claim element (examples denoted below by underlining)[7];
- by such excessive disclaimers of specificity of a term that the term becomes meaningless;
- by inconsistent uses of a term within a single specification;
- by inconsistent uses of a term between a specification and something allegedly incorporated into that specification;
- by inconsistencies within the language of a given claim;

This lack of definiteness is exacerbated by InterTrust trying to apply these claims to the very different structures and techniques of (or that InterTrust mistakenly attributes to) Microsoft's accused software. Particularly in view of these untenable infringement accusations, the following bolded claim terms and phrases are indefinite under 35 U.S.C. § 112, ¶ 2. Microsoft reserves the

---

[6] For ease of reference only, the accompanying claim listings use the clause numbering and lettering used by InterTrust in its PLR 3-1 Statements.

[7] Other undefined, indefinite claim terms are so ambiguous that one or more possible constructions are purely functional such that the term, as so construed, is a Section 112, ¶ 6 limitation. Microsoft, therefore, reserves the right to identify additional claim limitations as

right to modify this listing, e.g., if and when InterTrust clarifies its infringement and claim construction positions.

'193

1) A method comprising:

a) **receiving** a digital **file including** music;

b) **storing** said digital **file in** a first **secure memory** of a first device;

c) **storing** information **associated with said digital file in a secure database** stored on said first device, said information **including** at least one **budget control** and at least one **copy control**, said at least one **budget control including** a **budget specifying the number of copies which can be made of said digital file**; and said at least one **copy control controlling the copies made of said digital file**;

d) **determining whether said digital file may be copied** and stored on **a second device based on at least said copy control**;

e) **if said copy control allows at least a portion of said digital file to be copied** and stored on **a second device**,

f) **copying at least a portion of** said digital **file**;

g) **transferring at least a portion** of said digital **file** to **a second device** including a **memory** and an **audio and/or video output**;

h) **storing** said digital **file in** said **memory** of said second device; and

i) including playing said music through **said audio output**.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file including** music;	- "receiving ... file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file." - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or

Section 112, ¶ 6, limitations.

	excludes merely holding a reference.
b) **storing** said digital **file in** a first **secure memory** of a first device;	- see above - "storing ... in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant"[8] SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
c) **storing** information **associated with said digital file in** a **secure database** stored on said first device,	- see above - if "associated with said digital file" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure

[8] Indefinite claim terms, such as "tamper-resistant," used in describing the indefiniteness of other claim terms, are used in their narrowest possible sense.

	database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** at least one **budget control**	- see above - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite. - "budget control" is not used in the specification and is indefinite.
and at least one **copy control,**	- see above - "copy control" is not used in the specification and is indefinite. For example, it is indefinite on whether "copy" is used as a verb or a noun. - "copy" is indefinite, e.g., on whether it encompasses or excludes something (or creating something) that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy."
said at least one **budget control including** a **budget specifying the number of copies which can be made of said digital file**;	- see above - "budget" is used inconsistently in the specification and is indefinite. For example, apparently it is used to refer sometimes to a "method," sometimes to a "component assembly," sometimes to a value, and sometimes to a UDE data structure. - "copies" is indefinite (see "copy" above) - if the phrase "specifying the number of copies which can be made of said digital file" is not at least limited to meaning the total global number of "copies" that ever will have been made of that "file" at any time, by any

	"user," by any device, and for any length of persistence, it would be indefinite.
and said at least one **copy control controlling the copies made of said digital file;**	- see above - if "controlling" is not at least limited to use of the disclosed "component assembly," "protected processing environment," "object registration," "secure container," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring that specific "controls" are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users," the term "controlling" would be indefinite. - the phrase "controlling the copies made of said digital file" is indefinite, e.g., on whether it refers to "controlling" the process of "copying" the "file," or "controlling" all resulting "copies" of the "file," or both.
d) **determining whether said digital file may be copied and stored on a second device based on at least said copy control;**	- see above - "copied" is indefinite (see "copy" above) - "determining whether said digital file may be copied and stored on a second device" is indefinite, e.g., on whether this step determines whether the "file" may be "copied" on a second device, on whether one or more determinations are made. - "a second device" is indefinite, e.g., on whether it means "any" second device or a particular second device. - depending on the construction of other claim limitations, such as "at least one copy control controlling the copies made of said digital file" the phrase "based on at least said copy control" may be inconsistent with other limitations of this claim and thus may be indefinite.
e) **if said copy control allows at least a portion of said digital file**	- see above - "a portion of said digital file" is indefinite, e.g., on

to be copied and stored on **a second device,**	whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "based on at least said copy control," the phrase "if said copy control allows" may be inconsistent with other limitations of this claim and thus may be indefinite. - depending on the construction of other claim limitations, such as "at least one copy control controlling the copies made of said digital file," the phrase "if said copy control allows at least a portion of said digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
f) **copying at least a portion of** said digital **file;**	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "copy control."
g) **transferring at least a portion** of said digital **file** to **a second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "copy control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or

	excludes a "portion" not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output**;	- "audio and/or video output" is indefinite, e.g., it is inconsistent with the later claim recitation of "said audio output."
h) **storing** said digital **file in** said **memory** of said second device; and	- see above
i) including playing said music through **said audio output**.	- "said audio output" is indefinite, e.g., it is inconsistent with the earlier claim recitation of "audio and/or video output."

2) A method as in claim 1, further comprising:

a) at **a time substantially contemporaneous with** said **transferring** step, recording in said first device **information indicating that said transfer has occurred**.

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

at **a time substantially contemporaneous with** said **transferring** step,	- see above - "a time substantially contemporaneous with" is not used in the specification, and is indefinite.
recording in said first device **information indicating that said**	- "transfer" is indefinite, e.g., on how it differs, if at all, from "move" or "copy."

transfer has occurred.	- "information indicating that said transfer has occurred" is indefinite, e.g., on the extent to which the information identifies "said transfer," e.g., what was "transferred" and/or to what it was "transferred."

3) A method as in claim 2, in which:

a) said **information indicating that said transfer has occurred includes** an **encumbrance on said budget**.

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) said **information indicating that said transfer has occurred includes** an **encumbrance on said budget.**	- see above - "an encumbrance on said budget" is indefinite, e.g., for the same reasons that "budget" is indefinite, and, as to its function and structure, and on whether it must be uniquely identifiable with respect to the universe of "VDE" nodes.

4) A method as in claim 3, in which:

a) said **encumbrance operates to reduce the number of copies of said digital file authorized by said budget**.

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

said **encumbrance operates to reduce the number of copies of said digital file authorized by said budget.**	- see above - "operates to reduce the number of copies of said digital file authorized by said budget" is indefinite, e.g., on whether it reduces the total global number of "copies" that ever will have been made of that "file" at any time,

	by any "user," by any device, and for any length of persistence, and on meaning of an "encumbrance" "operating."

11) A method comprising:

2. **receiving** a digital **file**;

b) **storing** said digital **file in** a first **secure memory** of a first device;

c) **storing** information **associated with said digital file in a secure database** stored on said first device, said information **including** a first **control**;

d) **determining whether said digital file may be copied and stored on a second device based on said first control, said determining step** including **identifying said second device** and determining whether said first **control** allows **transfer** of **said copied file** to said second device, **said determination** based at least in part on **the features present at the device to which said copied file is to be transferred**;

e) **if said first control allows at least a portion of said digital file to be copied and stored on a second device**,

f) **copying at least a portion** of said digital **file**;

g) **transferring at least a portion** of said digital **file to a second device** including a **memory** and an **audio and/or video output**;

h) **storing said digital file in** said **memory** of said second device; and

2. **rendering said digital file** through said output.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file**;	- "receiving ... file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) **storing** said digital **file in** a first **secure memory** of a first	- see above - "storing ... in" is used inconsistently in the

device;	specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant" SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
c) **storing** information **associated with said digital file in** a **secure database** stored on said first device,	- see above - if "associated with said digital file" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** a first **control**	- see above - "including" is used inconsistently in the specification

	and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
d) **determining whether said digital file may be copied and stored on a second device based on said first control**;	- see above - "copied" is indefinite (see "copy" above) - "determining whether said digital file may be copied and stored on a second device" is indefinite, e.g., on whether this step determines whether the file may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it means "any" second device or a particular second device. - "determining whether said digital file may be copied and stored on a second device based on said first control" is indefinite; e.g., it is inconsistent with the later claim limitation "if said first control allows at least a portion of said digital file to be copied and stored on a second device"
said determining step including **identifying said second device** and determining whether said first **control** allows **transfer** of **said copied file** to said second device,	- see above - "identifying said second device" is indefinite, e.g., on whether the identification is of the type of device or of the particular second device unit, and on whether it is a unique identification. - "transfer" is indefinite, e.g., on how it differs, if at all, from "move" or "copy." - "said copied file" lacks antecedent basis, and is indefinite. For example, the preceding limitations do not recite the "copying" of any "file" that could be an

	antecedent for " said copied file." - if "copied file" is not at least limited to a "file" that has been "copied" at least once, then "copied file" would be indefinite.
said determination based at least in part on **the features present at the device to which said copied file is to be transferred**;	- "said determination" is indefinite as to its antecedent basis (e.g., "determining whether said digital file may be copied and stored ..." or "determining whether said first control allows transfer ...."). - "the features present at the device" is indefinite, e.g., on whether "the features" means all or any particular type of features, on what has these "features," and on the relationship, if any, of "features present at the device" to features of the device. - "to which said copied filed is to be transferred" is indefinite. For example, it is inconsistent with the other claim limitations reciting that "transfer" may not be allowed. - "transferred" is indefinite, e.g., on how it differs, if at all, from "moved."
e) **if said first control allows at least a portion of said digital file to be copied** and stored on **a second device**,	- see above - "a portion of said digital file" is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the "file." - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the "said second device" recited earlier in the claim. - depending on the construction of other claim limitations, such as "determining whether said digital file may be copied and stored on a second device based on said first control," the phrase "if said first control allows at least a portion of said digital file to be copied and stored on a second device" may be inconsistent with

	other limitations of this claim, and thus may be indefinite.
f) **copying at least a portion** of said digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control."
g) **transferring at least a portion** of said digital **file to a second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the "said second device" recited earlier in the claim.
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output**;	- "audio and/or video output" is indefinite.
h) **storing said digital file in** said **memory** of said second device;	- see above - "storing said digital file" is indefinite and

and	inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."
i) **rendering said digital file** through **said output**.	- see above - "rendering said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."

15) A method comprising:

2. **receiving** a digital **file**;

b) an **authentication step** comprising:

c) **accessing** at least one **identifier associated with a first device**; and

d) **determining whether said identifier is associated with a device and/or user authorized to store said digital file**;

e) **storing** said digital **file in** a first **secure memory** of said first device, **but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized**;

f) **storing** information **associated with said digital file in a secure database** stored on said first device, said information **including** at least one **control**;

g) **determining whether said digital file may be copied and stored on a second device based on said at least one control**;

h) **if said at least one control allows at least a portion of said digital file to be copied** and stored on **a second device**,

2. **copying at least a portion** of said digital **file**;

j) **transferring at least a portion** of said digital **file** to a **second device** including a **memory** and an **audio and/or video output**;

k) **storing said digital file in** said **memory** of said second device; and

l) **rendering said digital file** through said output.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file**;	- "receiving ... file" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "file," and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) an **authentication step** comprising:	- "authentication step" is indefinite, e.g., for the reasons set forth below.
c) **accessing** at least one **identifier associated with a first device or with a user of said first device**; and	- "accessing" is indefinite, e.g., on whether it encompasses or excludes ascertaining the information content of what is "accessed" (e.g., decrypting any encrypted information). - if "identifier" is not at least limited to a value that uniquely identifies a particular device or "user," it would be indefinite. - "identifier associated with" is indefinite, e.g., on whether the "identifier" is uniquely "associated with." - "identifier associated with a first device or with a user of said first device" is indefinite and inconsistent with the later claim recitation of "determining whether said identifier is associated with a device and/or user ...." - "a user of said first device" is indefinite, e.g., on whether the "user" is a current, past, or potential "user" of the device.
d) **determining whether said identifier is associated with a device and/or user authorized to store said digital file**;	- "determining whether said identifier is associated with a device and/or user" is indefinite and inconsistent with the preceding claim limitation of an "identifier associated with a first device or with a user of said first device." - "authorized to store said digital file" is indefinite, e.g., on whether such "authorization" is conditional or

	unconditional.
e) **storing** said digital **file in** a first **secure memory** of said first device,	- see above - "storing ... in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - if "secure memory" is not at least limited to the disclosed internal RAM and/or ROM (directly addressable by a SPU processor instruction) located within the physically protected, "tamper-resistant" SPU, the term "secure memory" would be indefinite. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure."
but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;	- "said device and/or user" is indefinite and has an indefinite antecedent basis (e.g., "a device and/or user authorized to store said digital file" or "at least one identifier associated with a first device or with a user of said first device"). - "so authorized" is indefinite and has an indefinite antecedent basis (e.g., "authorized" for "storing said digital file in a first secure memory of said first device" or "authorized to store said digital file"). - "but only if said device and/or user is so authorized" is inconsistent with "but not proceeding with said storing if said device and/or user is not authorized," rendering both phrases indefinite.
f) **storing** information **associated with said digital file in a secure**	- see above - if "associated with said digital file" is not at least

database stored on said first device,	limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with said digital file" would be indefinite. - if "secure database" is not at least limited to the disclosed "secure database" (including its "secure database manager" and alleged access control "VDE" mechanisms), the term "secure database" would be indefinite.
said information **including** at least one **control**	- see above - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
g) **determining whether said digital file may be copied and stored on a second device based on said at least one control**;	- see above - "copied" is indefinite (see "copy" above) - "determining whether said digital file may be copied and stored on a second device based on said at least one control" is indefinite, e.g., on whether this step determines whether the "file" may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it

	means "any" second device or a particular second device.
h) **if said at least one control allows at least a portion of said digital file to be copied** and stored on **a second device**,	- see above - "a portion of said digital file" is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "determining whether said digital file may be copied and stored on a second device based on said at least one control," the phrase "if said at least one control allows at least a portion of said digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
i) **copying at least a portion** of said digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "at least one control."
j) **transferring at least a portion** of said digital **file** to a **second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "at least one control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "copied" in the preceding step.

	- "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
and an **audio and/or video output**;	- "audio and/or video output" is indefinite.
h) **storing said digital file in** said **memory** of said second device; and	- see above - "storing said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."
i) **rendering said digital file** through **said output**.	- see above - "rendering said digital file" is indefinite and inconsistent with other claim limitations, e.g., "transferring at least a portion of said digital file to a second device."

19) A method comprising:

a) **receiving** a digital **file at** a first device;

b) **establishing communication between** said first device and a **clearinghouse** located at a **location remote from** said first device;

c) said first device obtaining **authorization information including** a key from said **clearinghouse**;

d) said first device using said **authorization information** to **gain access to or** make at least one **use** of said first digital **file**, including using said key to decrypt at least a portion of said first digital **file**; and

e) **receiving** a first **control** from said **clearinghouse at** said first device;

f) **storing** said first digital **file in** a **memory** of said first device;

g) using said first **control** to **determine whether said first digital file may be copied and stored on a second device**;

h) **if said first control allows at least a portion of said first digital file to be copied** and stored on **a second device,**

i) **copying at least a portion** of said first digital **file**;

j) **transferring at least a portion** of said first digital **file** to a **second device** including a **memory** and an **audio and/or video output**;

k) **storing** said first digital **file portion in** said **memory** of said second device; and

l) rendering said first digital **file portion** through **said output**.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

a) **receiving** a digital **file at** a first device;	- "receiving ... at" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, and on what or where it is received from. - "file" is indefinite, e.g., on whether it encompasses or excludes a duplicate or "copy" of the "file."
b) **establishing communication between** said first device and a **clearinghouse** located at a **location remote from** said first device;	- "establishing communication between" is indefinite, e.g., on whether this step requires one or more "communications," on whether two-way "communication" must be established, and on the nature of the "communication." - "location remote from" is indefinite, e.g., on how "remoteness" is determined. - "clearinghouse" is indefinite. For example, it vaguely suggests a function without suggesting any particular structure for performing such function. No particular corresponding structure is adequately described in the specification.
c) said first device obtaining	- if "authorization information" is not at least limited

authorization information including a key from said **clearinghouse**;	to (1) the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, and (2) the key and other data used thereby, the term "authorization information" would be indefinite. - "including" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference.
d) said first device using said **authorization information** to **gain access to or** make at least one **use** of said first digital **file**, including using said key to decrypt at least a portion of said first digital **file**; and	- "gain access to" is indefinite, e.g., on whether it encompasses or excludes ascertaining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying."
e) **receiving** a first **control** from said **clearinghouse** at said first device;	- see above - "control" is used inconsistently in the specification. If "control" is not at least limited to the disclosed executable, modular "component assembly" component that, inter alia, performs its "VDE" "access control" tasks at an arbitrary granular level, the term "control" would be indefinite.
f) **storing** said first digital **file in** a **memory** of said first device;	- see above - "storing ... in" is used inconsistently in the specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor.
g) using said first **control** to **determine whether said first**	- see above - "copied" is indefinite, e.g., on whether it

digital file may be copied and stored on a second device;	encompasses or excludes creating something that is not an identical duplicate of the original; and if it does encompass that, then how clear that something must be to the original to constitute a "copy." - "determine whether said first digital file may be copied and stored on a second device" is indefinite, e.g., on whether this step determines whether the "file" may be "copied" on a second device. - "a second device" is indefinite, e.g., on whether it means "any" second device or a particular second device. - "using said first control to determine whether said first digital file may be copied and stored on a second device" is indefinite; e.g., it is inconsistent with the later claim limitation "if said first control allows at least a portion of said first digital file to be copied and stored on a second device"
h) **if said first control allows at least a portion of said first digital file to be copied and stored on a second device,**	- see above - "a portion of said digital file" is indefinite, e.g., on whether it encompasses or excludes matter that is merely referenced within the "file." - depending on the construction of other claim limitations, such as "using said first control to determine whether said first digital file may be copied and stored on a second device" the phrase "if said first control allows at least a portion of said first digital file to be copied" may be inconsistent with other limitations of this claim, and thus may be indefinite.
i) **copying at least a portion** of said first digital **file**;	- see above - "copying" is indefinite, e.g., on whether it encompasses or excludes creating something that is not an identical duplicate of the original; and, if it does encompass that, then how close that something must be

	to the original to constitute a "copy." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control."
j) **transferring at least a portion** of said first digital **file** to a **second device**	- see above - "transferring" is indefinite, e.g., on how it differs, if at all, from "moving" or "copying." - "at least a portion" is indefinite and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a "portion" not "allowed" "to be copied and stored on a second device" by the "first control." - "at least a portion" is indefinite, and has an indefinite antecedent basis, e.g., on whether it encompasses or excludes a portion not "copied" in the preceding step. - "a second device" is indefinite, and has an indefinite antecedent basis, e.g., on whether it is limited to the same particular second device referred to earlier in the claim (to the extent the claim earlier refers to a particular second device).
including a **memory**	- see above
and an **audio and/or video output**;	- "audio and/or video output" is indefinite.
k) **storing** said first digital **file portion in** said **memory** of said second device; and	- see above
l) rendering said first digital **file portion** through **said output**.	- see above

'683

2. A system including:

a **first apparatus including,**

user controls,

a communications port,

a processor,

a **memory storing**:

a first **secure container containing a governed item**, the first **secure container governed item** being at least in part encrypted; the first **secure container having been received from a second apparatus**;

a first **secure container rule at least in part governing an aspect of access to or use of** said first **secure container governed item, the first secure container rule**, the first **secure container rule having been received from a third apparatus** different from said second apparatus; and

hardware or software used for receiving and opening secure containers,said secure containers each **including the capacity to contain a governed item**, a **secure container rule being associated with** each of **said secure containers**;

a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus**, said **protected processing environment** including **hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

2. A system including:	
a **first apparatus including,**	- the claim is indefinite on which of the recited elements are included in the "first apparatus."
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory storing**:	- "memory" is indefinite, e.g., on whether it

	encompasses or excludes storage that is not directly addressable by the processor. - "storing" is used inconsistently in at least the allegedly incorporated specification and is indefinite, e.g., on whether it encompasses or excludes merely holding a reference. - the claim is indefinite on which of the recited elements are "stored" in the "memory."
a first **secure container containing a governed item**,	- "secure container" is indefinite, e.g., on its structure and certain of its functions, on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "container" is indefinite, e.g., on its structure and certain of its functions, and on what distinguishes a single "container" from two separate "containers." - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure." - "storing ... secure container" is indefinite, e.g., on what part, if any, of the "container" may merely be referenced from within the memory. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing."

	- if "govern" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the term "governed" (and "governed item") would be indefinite. - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate governed items.
the first **secure container governed item** being at least in part encrypted;	- see above
the first **secure container having been received from a second apparatus**;	- see above - "received" is indefinite, e.g., on what processing, if any, is required to complete this "receipt," and on what "received" the "received" item. - "having been received from" recites the (possibly unknowable) history of a component (or something stored in a component) rather than the structure or function of the component, apparatus or system, thereby rendering this apparatus claim indefinite. - "received from a second apparatus" is indefinite, e.g., on whether this encompasses or excludes receipt from some intermediary between the second apparatus and first apparatus.
a first **secure container rule at least in part governing an**	- see above - "rule" is indefinite and is used inconsistently in the

aspect of access to or use of said first **secure container governed item,**	specification. For example, the relationship between a "rule" and a "control" is indefinite. - "secure container rule" is indefinite and not used in the specification. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "governing." - if "governing" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the term "governing" would be indefinite. - "at least in part governing" is indefinite, e.g., on how to identify when this act of "governing" has begun, is ongoing, or has ended. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite.
the first secure container rule,	- see above - the claim is indefinite on the significance of this repetition of the phrase "the first secure container rule."

the first **secure container rule having been received from a third apparatus** different from said second apparatus; and	- see above - "received from a third apparatus" is indefinite, e.g., on whether this encompasses or excludes receipt from some intermediary between the third apparatus and first apparatus.
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same "hardware or software" performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.
said secure containers each **including the capacity to contain a governed item,**	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does

	encompass merely holding a reference, what type of reference suffices to constitute "contain." - "including the capacity to contain a governed item" is indefinite, e.g., on the manner in which a "capacity" is included in a "secure container," and on whether the "capacity to contain" must apply to some particular "governed item" or to every "governed item" without limitation.
a **secure container rule being associated with** each of **said** **secure containers**;	- see above - if "being associated with ... secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific users, the phrase "being associated with ... secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,**	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?), and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected."

	- if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a "protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from ... tampering" is indefinite, e.g., on the specific threat(s) being addressed, and on the level(s) and nature of protection from those threats. - "a user of said first apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user."

said **protected processing environment** including **hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and	- see above - "said first secure container rule and a second secure container rule" is indefinite, e.g., on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying ... in a secure container" is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying ... in combination" is indefinite, e.g., on the manner in which the "rules" are merged and applied. - "contained in" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference in, and, if it does encompass merely holding a reference in, what type of reference suffices to constitute "contained in." - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "govern" would be indefinite. - "a governed item contained in a secure container" is indefinite and has no or an indefinite antecedent basis as both "a governed item" and "a secure container."

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	- see above - "hardware or software used for transmission ... or for the receipt ... from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," and on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.

28. A system including;

a **first apparatus including**;

user controls,

a communications port,

a processor,

a **memory containing a** first **rule,**

hardware or software used for receiving and opening secure containers,said secure containers each **including the capacity to contain a governed item,** a **secure container rule being associated with** each of **said secure containers**;

a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,** said **protected processing environment** including **hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

a **second apparatus including**:

user controls,

a communications port,

a processor,

a **memory containing a** second **rule,**

hardware or software used for receiving and opening secure containers,**said secure containers** each **including the capacity to contain a governed item, a secure container rule being associated with** each of **said secure containers**;
a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus**, said **protected processing environment** including **hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**;
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and
an **electronic intermediary**, said **intermediary** including a **user rights authority clearinghouse**.

Following are some examples of the many ways in which this claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

28. A system including:	
a **first apparatus including,**	- the claim is indefinite on which of the recited elements are included in the "first apparatus."
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory containing a** first **rule,**	- "memory" is indefinite, e.g., on whether it encompasses or excludes storage that is not directly addressable by the processor. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing." - "rule" is indefinite and is used inconsistently in the specification. For example, the relationship between a

	"rule" and a "control" is indefinite.
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "secure container" is indefinite, e.g., on its structure and certain of its functions, and on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "container" is indefinite, e.g., on its structure and certain of its functions, and on what distinguishes a single "container" from two separate "containers." - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "secure" from "not secure." - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same "hardware or software" performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.

said <u>secure containers</u> each **including the capacity to contain a governed item,**	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate "governed items." - "including the capacity to contain a governed item" is indefinite.
a secure container rule being associated with each of **said <u>secure containers</u>**;	- see above - if "associated with ... secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with ... secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able

	to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected." - if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a

	"protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from ... tampering" is indefinite, e.g., on the specific threat(s) being addressed and on the level(s) and nature of protection from those threats. - "a user of said first apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user."
said **protected processing environment** including **hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and	- see above - "said first rule and a secure container rule" is indefinite, e.g., on whether "a secure container rule" is separate from a "first rule," and on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying ... in a secure container," is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying ... in combination" is indefinite, e.g., on the manner in which the "rules" are merged and applied. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing unapproved user processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular

	level), and specific "users," the term "govern" would be indefinite. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is accessed (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite. - "a governed item" is indefinite and has no or an indefinite antecedent.
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	- see above - "hardware or software used for transmission ... or for the receipt ... from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," on whether the same "hardware or software" performs both, and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.
a **second apparatus including**,	- the claim is indefinite on which of the recited elements are included in the "second apparatus." - the claim is indefinite for failing to link the first apparatus with the second apparatus in any manner.
user controls,	- "user controls" is indefinite.
a communications port,	
a processor,	
a **memory containing a** second	- "memory" is indefinite, e.g., on whether it

rule,	encompasses or excludes storage that is not directly addressable by the processor. - "containing" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "containing." - "rule" is indefinite and is used inconsistently in the specification. For example, it is indefinite on what distinguishes a single "rule" from two separate "rules."
hardware or software used for receiving and opening secure containers,	- see above - "receiving" is indefinite, e.g., on what processing, if any, is required to complete this "receiving" step, on what receives the "secure containers," and on what or where they are received from. - if "opening secure containers" is not at least limited to successful completion of the "OPEN method" expressly disclosed in the allegedly incorporated specification, the phrase "opening secure containers" would be indefinite. - "secure container" is indefinite, e.g., on its structure and certain of its functions, and on whether it encompasses or excludes "virtual container." The specification does not disclose adequate corresponding structure under Section 112, ¶ 6. - "secure" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from

	those threats that separate(s) "secure" from "not secure." - "hardware or software used for receiving and opening secure containers," is indefinite, e.g., on the structure of this "hardware or software," and on whether the same hardware or software performs both "receiving" and "opening." The specification does not disclose adequate corresponding structure.
said <u>secure containers</u> each **including the capacity to contain a governed item,**	- see above - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" would be indefinite. - "contain" is indefinite and used inconsistently in at least the allegedly incorporated specification. For example, it is indefinite on whether it encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "a governed item," is indefinite, e.g., on what distinguishes "a governed item" from two separate governed items. - "including the capacity to contain a governed item" is indefinite.
a **secure container rule being associated with** each of **said <u>secure containers</u>**;	- see above - if "associated with ... secure containers" is not at least limited to use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between

	specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the phrase "associated with ... secure containers" would be indefinite. - if "said secure containers" is not at least limited to all "secure containers" which the "hardware or software used for receiving and opening secure containers" is able to "receive and open" (regardless of whether it has done so), the phrase "said secure containers" is indefinite.
a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus,**	- "protected" is indefinite. It is an amorphous term that the specification both fails to define and uses inconsistently. For example, it is indefinite on what sort of threat(s) is (are) being addressed (e.g., confidentiality? integrity? authentication? non-repudiation? availability?) and on the nature and the level(s) of protection from those threats that separate(s) "protected" from "not protected." - if "protected processing environment" is not at least limited to excluding the processor and "memory" recited earlier in the claim, and is not at least limited to executing software and/or hardware (if any) expressly disclosed in the specification and identified as a "protected processing environment," the term "protected processing environment" would be indefinite. - if "protecting" is not at least limited to preventing unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific

	"objects" (and their content at an arbitrary granular level), and specific "users," the term "protecting" would be indefinite. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "protecting." - "information contained in said protected processing environment" is indefinite, e.g., on what aspects of a "protected processing environment" can "contain" information, and on whether "contain" encompasses or excludes merely holding a reference, and, if it does encompass merely holding a reference, what type of reference suffices to constitute "contain." - "protecting from ... tampering" is indefinite, e.g., on the specific threat(s) being addressed and on the level(s) and nature of protection from those threats. - "a user of said apparatus" is indefinite, e.g., on whether "a user" means "any user" or a particular "user," and on whether "said apparatus" is the first or second apparatus.
said **protected processing environment** including **hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and	- see above - "said second rule and a secure container rule" is indefinite, e.g., on what distinguishes a single "rule" from two separate "rules." - "hardware or software used for applying ... in a secure container," is indefinite, e.g., on the structure of this "hardware or software." The specification does not disclose adequate corresponding structure. - "applying ... in combination" is indefinite, e.g., on the manner in which the rules are merged and applied. - "at least in part" is indefinite, and, under some possible meanings, inconsistent with "govern." - if "govern" is not at least limited to preventing

	unauthorized "user" processing of a particular item on a per item basis by use of the disclosed "component assembly," "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users," the term "govern" would be indefinite. - "access" is indefinite, e.g., on whether it encompasses or excludes determining the information content of what is "accessed" (e.g., decrypting any encrypted information). - "use" is indefinite and is used inconsistently in the allegedly incorporated specification, e.g., on whether or not it encompasses or excludes "distribution," "extraction," "manipulating," and/or "copying." - "an aspect of access to or use of" is indefinite. - "a governed item" is indefinite and has no or an indefinite antecedent.
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	- see above - "hardware or software used for transmission ... or for the receipt ... from other apparatuses" is indefinite, e.g., on the structure of this "hardware or software," and on its relationship, if any, with the previously recited "hardware or software used for receiving and opening secure containers," and on its relationship, if any, with any other element recited in the claim. The specification does not disclose adequate corresponding structure.
an **electronic intermediary**, said **intermediary** including a **user**	- see above - "electronic intermediary" is indefinite, e.g., as to the

rights authority clearinghouse.	nature of its structure and function, and its relationship, if any, to either the first apparatus or the second apparatus, or to any other element of the claim, and on whether it encompasses or excludes a "virtual intermediary" or "virtual go-between." The specification does not disclose adequate corresponding structure. - "rights" is indefinite. - "user rights authority clearinghouse" is indefinite, e.g., as to the nature of its structure and function, and its relationship, if any, to either the first apparatus or the second apparatus, or to any other element of the claim. The specification does not disclose adequate corresponding structure.

29. A system as in claim 28, said **user rights authority clearinghouse operatively connected to make rights available to users.**

Following are some examples of the additional ways in which this dependent claim and these claim terms and phrases are indefinite on the face of the patent and/or as apparently construed by InterTrust:

A system as in claim 28, said **user rights authority clearinghouse operatively connected to make rights available to users.**	- see above - "operatively connected" is indefinite, e.g., as to what it is connected. - "to make rights available to users" is indefinite, e.g., on which "users" it addresses and what it means for "rights" to be "available" to those "users."

Enablement and Written Description
Invalidity of the Asserted InterTrust Patent Claims

Each of the asserted InterTrust patent claims is invalid for violating the written description and enablement requirements of 35 U.S.C. § 112, ¶ 1, particularly as the claims are construed in the untenable manner apparently underlying InterTrust's infringement accusations in this action.

One way in which the claims of the '193 patent and the '683 patent (including but not limited to the extent the allegedly incorporated applications are considered) are not enabled is that the applications from which they issued are so rambling, unfocused, vague and internally inconsistent that they obfuscated any alleged teaching of the claimed subject matter and failed to enable one of skill in the art, without undue experimentation, to follow any alleged directions of the application to carry out the claimed subject matter.

The claims are invalid for violating the written description requirement to the extent that they are construed so as to contradict and/or not require the essential, non-optional alleged attributes of the alleged "invention" that were identified in the application (as originally filed, disregarding all new matter) from which the claims issued. Those disclosed "invention" defining statements include descriptions of the "present invention" and/or "VDE" or "virtual distribution environment," statements distinguishing prior techniques or products, such statements in the Summary of the Invention or Objects of the Invention sections of the application, and non-optional attributes shared by the disclosed embodiments and/or initial application claims. They include, but are not limited to, such alleged attributes reflected in the below-listed exemplary statements in the applications filed on December 9, 1998 (the '193 Patent), December 28, 1998 (the '683 Patent), and/or similar statements in the patents' Patent Office prosecution histories and/or any properly incorporated patent(s) or patent application(s), if any.

The claims are further invalid under the enablement requirement as the applications did not enable those of skill in the art to build systems having these touted attributes, at least not without an unreasonable amount of experimentation.

- "The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway."

- "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted

by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems."

- "VDE may be used to provide basic usage control in several ways. First, it permits the "embedding" of multiple containers within a single object. Embedded objects permit the "nesting" of control structures within a container. VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and provides flexible control information over any action associated with the information which can be described as a VDE controlled process."

- "Providers of "electronic currency" have also created protections for their type of content. These systems are not sufficiently adaptable, efficient, nor flexible enough to support the generalized use of electronic currency. Furthermore, they do not provide sophisticated auditing and control configuration capabilities. This means that current electronic currency tools lack the sophistication needed for many real- world financial business models. VDE provides means for anonymous currency and for "conditionally" anonymous currency, wherein currency related activities remain anonymous except under special circumstances."

- "Traditional content control mechanisms often require users to purchase more electronic information than the user needs or desires. For example, infrequent users of shrink-wrapped software are required to purchase a program at the same price as frequent users, even though they may receive much less value from their less frequent use. Traditional systems do not scale cost according to the extent or character of usage and traditional systems can not attract potential customers who find that a fixed price is too high. Systems using traditional mechanisms are also not normally particularly secure. For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package."

- "Traditional electronic information rights protection systems are often inflexible and inefficient and may cause a content provider to choose costly distribution channels that increase a product's price. In general these mechanisms restrict product pricing, configuration, and marketing flexibility. These compromises are the result of techniques for controlling information which cannot accommodate both different content models and content models which reflect the many, varied requirements, such as content delivery strategies, of the model participants. This can

limit a provider's ability to deliver sufficient overall value to justify a given product's cost in the eyes of many potential users. VDE allows content providers and distributors to create applications and distribution networks that reflect content providers' and users' preferred business models. It offers users a uniquely cost effective and feature rich system that supports the ways providers want to distribute information and the ways users want to use such information."

- "VDE provides important enhancements for improving data security in organizations by providing "smart" transaction management features that can be far more effective than key and password based "go/no go" technology."

- "A variety of capabilities are required to implement an electronic commerce environment. VDE is the first system that provides many of these capabilities and therefore solves fundamental problems related to electronic dissemination of information."

- "The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability amongst devices functioning in electronic commerce and/or data security environments."

- "Templates, classes (including user groups employing an object under group access), and flexible control structures including object "independent" permissions records (permissions that can be associated with a plurality of objects) and structures that support budgeting and auditing as separate VDE processes, help focus the flexible and configurable capabilities inherent within authoring provided by the present invention in the context of specific industries and/or businesses and/or applications. ... The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, ... the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances."

- "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable."

- "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function."

- "A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). This shaping can occur as content control information passes from one VDE participant to another and to the extent allowed by "in place" content control information. This process allows users of VDE to recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements)."

- "VDE's fundamental configurability will allow a broad range of competitive electronic commerce business models to flourish."

- "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/or otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well."

- "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content

containers. Such capabilities allow VDE supported product models to evolve by progressively reflecting the requirements of "next" participants in an electronic commercial model."

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security;"

- "Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (c) generic content model;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (b) modular data structures;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (d) general modularity and independence of foundation architectural components;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (e) modular security structures;"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (f) variable length and multiple branching chains of control; and"

- "Some of the key factors contributing to the configurability intrinsic to the present invention include: (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling."

- "An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that: ... "sufficiently" impede unauthorized and/or uncompensated use of electronic information and/or appliances through the use of secure communication, storage, and transaction management technologies ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support low-cost, efficient, and effective security architectures for transaction control, auditing, reporting, and related communications and information storage ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... securely store at a user's site potentially highly detailed information reflective of a user's usage of a variety of different content segment types... support trusted chain of handling capabilities for pathways of distributed electronic information and/or for content usage related information."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support flexible auditing mechanisms, such as employing "bitmap meters, ..."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support "launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the content to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... securely support electronic currency and credit usage control, storage, and communication at, and between, VDE installations."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide smart object agents that can carry requests, data, and/or methods, including budgets, authorizations, credit or currency, and content. ... Smart objects can, for example, be transmitted to a remote location to perform a specified database search on behalf of a user ...."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic

commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... "employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses. ...Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by "typical" users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that VDE related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security risks associated with possible presence of viruses in such modules. ... As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities. ... Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such

as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enables users ... to specify preferences or requirements related to their use of electronic content and/or appliances. Content users, such as end-user customers using commercially distributed content ... can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content. Uses include, for example, a user setting a limit on the price for electronic documents that the user is willing to pay without prior express user authorization, and the user establishing the character of metering information he or she is willing to allow to be collected (privacy protection)."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms that allow control information to "evolve" and be modified according, at least in part, to independently, securely delivered further control information. ... Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content)."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for

concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process."

- "it is important to provide a framework of operation and/or structure to allow existing industries and/or applications and/or businesses to manipulate familiar concepts related to content types, distribution approaches, pricing mechanisms, user interactions with content and/or related administrative activities, budgets, and the like."

- "The present invention allows content providers and users to formulate their transaction environment to accommodate:

- (1) desired content models, content control models, and content usage information pathways,

- (2) a complete range of electronic media and distribution means,

- (3) a broad range of pricing, payment, and auditing strategies,

- (4) very flexible privacy and/or reporting models,

- (5) practical and effective security architectures, and

- (6) other administrative procedures that together with steps (1) through (5) can enable most "real world" electronic commerce and data security models, including models unique to the electronic world."

- "This ability of the present invention to support multiple pathway branches for the flow of both VDE content control information and VDE managed content enables an electronic

commerce marketplace which supports diverging, competitive business partnerships, agreements, and evolving overall business models which can employ the same content properties combined, for example, in differing collections of content representing differing at least in part competitive products."

- "the present invention can help ensure, for example, that parties, will be paid for use of distributed information in a manner consistent with their agreement; ... the present invention can, for example, help ensure that data is used only in authorized ways; ...."

- "The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, to allow for efficient adaptation into new industries as they evolve, and to reflect the evolution and/or change of an existing industry and/or business, as well as to support one or more groups of users who may be associated with certain permissions and/or budgets and object types. The flexibility of VDE templates, classes, and basic control structures is enhanced through the use of VDE aggregate and control methods which have a compound, conditional process impact on object control. Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment. Thus, the present invention fully supports the requirements and biases of content providers without forcing them to fit a predefined application model. It allows them to define the rights, control information, and flow of their content (and the return of audit information) through distribution channels."

- "a creator ... may allow changes by an auditor for event trails, but not allow anyone but themselves to read those trails ...."

- "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. As a result, the creator and/or distributor and/or client administrator and/or other contributor of secure control information for each property (for example, an end-user restricting the kind of audit information he or she will allow to be reported and/or a financial clearinghouse establishing certain criteria for use of its credit for payment for use of distributed content) can be confident that their contributed and

accepted control information will be enforced (within the security limitations of a given VDE security implementation design)."

- "Since different groups of components can be put together for different applications, the present invention can provide electronic control information for a wide variety of different products and markets. This means the present invention can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as a single standard for electronic rights protection, data security, and electronic currency and banking."

- "In a VDE, the separation between a rights application and its foundation permits the efficient selection of sets of control information that are appropriate for each of many different types of applications and uses."

- "Due to its open design, VDE allows (normally under securely controlled circumstances) applications using technology independently created by users to be "added" to the system and used in conjunction with the foundation of the invention."

- "In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity."

- "VDE permits multiple, separate electronic arrangements to be formed between subsets of parties in a VDE supported electronic value chain model. These multiple agreements together comprise a VDE value chain "extended" agreement. VDE allows such constituent electronic agreements, and therefore overall VDE extended agreements, to evolve and reshape over time as additional VDE participants become involved in VDE content and/or appliance control information handling. VDE electronic agreements may also be extended as new control information is submitted by existing participants. With VDE, electronic commerce participants are free to structure and restructure their electronic commerce business activities and relationships. As a result, the present invention allows a competitive electronic commerce marketplace to develop since the use of VDE enables different, widely varying business models using the same or shared content."

- "A feature of the present invention enables such flexibility of metering control mechanisms to accommodate a simultaneous, broad array of: (a) different parameters related to electronic information content use; (b) different increment units (bytes, documents, properties, paragraphs, images, etc.) and/or other organizations of such electronic content; and/or (c) different categories of user and/or VDE installation types, such as client organizations, departments, projects, networks, and/or individual users, etc. This feature of the present invention can be employed for ...."

- "A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit."

- "Features of the present invention help ensure that a requirement that a clearinghouse report such usage information and payment content will be observed."

- "A feature of the present invention is the use of portable VDEs as transaction cards at retail and other establishments, wherein such cards can "dock" with an establishment terminal that has a VDE secure sub-system and/or an online connection to a VDE secure and/or otherwise secure and compatible subsystem, such as a "trusted" financial clearinghouse (e.g., VISA, Mastercard)."

- "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content. For example, a distributor of a certain type of content might be allowed by "senior" participants (by content creators, for example) to require a method which prohibits end-users from electronically saving decrypted content, a provider of credit for VDE transactions might require an audit method that records the time of an electronic purchase, and/or a user might require a method that summarizes usage information for reporting to a clearinghouse (e.g. billing information) in a way that does not convey confidential, personal information regarding detailed usage behavior. A further feature of VDE provided by the present invention is that creators, distributors, and users of content can select from among a set of predefined methods (if available) to control container content usage and distribution functions and/or they may have the right to provide new customized methods to control at least certain usage functions (such "new" methods may be required to be certified for trustedness and interoperability to the VDE installation and/or for of a group of VDE applications). As a result, VDE provides a very high degree of

configurability with respect to how the distribution and other usage of each property or object (or one or more portions of objects or properties as desired and/or applicable) will be controlled."

- "the present invention's trusted/secure, universe wide, distributed transaction control and administration system."

- "The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications."

- "Templates, classes (including user groups employing an object under group access), and flexible control structures including object "independent" permissions records (permissions that can be associated with a plurality of objects) and structures that support budgeting and auditing as separate VDE processes, help focus the flexible and configurable capabilities inherent within authoring provided by the present invention in the context of specific industries and/or businesses and/or applications. ... The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, ... the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment."

- "As with the content control information for most VDE managed content, features of the present invention allows [sic] the content's control information to: (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. ... (b) allow a user to combine additional content with at least a portion of said extracted content, ... (c) allow a user to securely edit at least a portion of said content while maintaining said content in a secure form within said VDE content container; ... (d) append extracted content to a pre-existing VDE content container object and attach associated control information ... (e) preserve VDE control over one or more portions of extracted content after various forms of usage of said portions ... Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected electronic content information extracted from content container sources while maintaining secure VDE

capabilities thus preserving the rights of providers in said content information after various content usage processes."

- "For example, features of the present invention include: (a) VDE system software to in part extend and/or modify host operating systems such that they possesses VDE capabilities, such as enabling secure transaction processing and electronic information storage; (b) one or more application programs that in part represent tools associated with VDE operation; and/or (c) code to be integrated into application programs, wherein such code incorporates references into VDE system software to integrate VDE capabilities and makes such applications VDE aware ...."

- "The distribution control information provided by the present invention allow flexible positive control. No provider is required to include any particular control, or use any particular strategy, except as required by senior control information. Rather, the present invention allows a provider to select from generic control components (which may be provided as a subset of components appropriate to a provider's specific market, for example, as included in and/or directly compatible with, a VDE application) to establish a structure appropriate for a given chain of handling/control."

- "In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification."

- "Control methods are created primarily through the use of one or more of said executable, reusable load module code pieces (normally in the form of executable object components) and associated data. The component nature of control methods allows the present invention to efficiently operate as a highly configurable content control system. Under the present invention, content control models can be iteratively and asynchronously shaped, and otherwise updated to accommodate the needs of VDE participants to the extent that such shaping and otherwise updating conforms to constraints applied by a VDE application, if any (e.g., whether new component assemblies are accepted and, if so, what certification requirements exist for such component assemblies or whether any or certain participants may shape any or certain control information by selection amongst optional control information (permissions record) control methods. This iterative (or concurrent) multiple participant process occurs as a result of the

submission and use of secure, control information components (executable code such as load modules and/or methods, and/or associated data)."

- "The special purpose secure circuitry provided by the present invention includes at least one of: a dedicated semiconductor arrangement known as a Secure Processing Unit (SPU) and/or a standard microprocessor, microcontroller, and/or other processing logic that accommodates the requirements of the present invention and functions as an SPU."

- "VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. VDE is not limited to being an application or application specific toolset that covers only a limited subset of electronic interaction activities and participants. Rather, VDE supports systems by which such applications can be created, modified, and/or reused. As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. VDE can support a single electronic "world" within which most forms of electronic transaction activities can be managed."

- "A fundamental problem for electronic content providers is extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, including use limitations, into an "extended" agreement comprising an overall electronic business model. This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations. Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE,

electronic commerce can function in the same way as traditional commerce-that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties."

- "VDE allows the owners and distributors of electronic digital information to reliably bill for, and securely control, audit, and budget the use of, electronic information. It can reliably detect and monitor the use of commercial information products."

- "VDE provides comprehensive and configurable transaction management, metering and monitoring technology."

- "Protecting the rights of electronic community members involves a broad range of technologies. VDE combines these technologies in a way that creates a "distributed" electronic rights protection "environment." This environment secures and protects transactions and other processes important for rights protection. VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes."

- "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users."

- "VDE provides a unified solution that allows all content creators, providers, and users to employ the same electronic rights protection solution. ... VDE can allow content to be exchanged "universally" and users of an implementation of the present invention can interact electronically without fear of incompatibilities in content control, violation of rights, or the need to get, install, or learn a new content control system."

- "In addition, VDE:

- (a) is very configurable, modifiable, and re-usable;

- (b) supports a wide range of useful capabilities that may be combined in different ways to accommodate most potential applications;

- (c) operates on a wide variety of electronic appliances ranging from hand-held inexpensive devices to large mainframe computers;

- (d) is able to ensure the various rights of a number of different parties, and a number of different rights protection schemes, simultaneously;

- (e) is able to preserve the rights of parties through a series of transactions that may occur at different times and different locations;

- (f) is able to flexibly accommodate different ways of securely delivering information and reporting usage; and

- (g) provides for electronic analogues to "real" money and credit, including anonymous electronic cash, to pay for products and services and to support personal (including home) banking and other financial activities."

• "Users of VDE will not require additional rights protection systems for different information highway products and rights problems--nor will they be required to install and learn a new system for each new information highway application... The content and control information supplied by one group can be used by people who normally use content and control information supplied by a different group. VDE can allow content to be exchanged "universally" and users of an implementation of the present invention can interact electronically without fear of incompatibilities in content control, violation of rights, or the need to get, install, or learn a new content control system."

• "[VDE] can protect electronic rights including: (d) the privacy rights of users of content, ..."

• "Secure VDE hardware (also known as SPUs for Secure Processing Units), or VDE installations that use software to substitute for, or complement, said hardware (provided by Host Processing Environments (HPEs)), operate in conjunction with secure communications, systems integration software, and distributed software control information and support structures, to achieve the electronic contract/rights protection environment of the present invention. Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment. In some embodiments and where commercially acceptable, certain VDE participants, such as clearinghouses that normally maintain sufficiently physically secure non-VDE processing environments, may be allowed to employ HPEs rather VDE hardware elements and interoperate, for example, with VDE end-users and content providers."

- "VDE provides generalized configurability. This results, in part, from decomposition of generalized requirements for supporting electronic commerce and data security into a broad range of constituent "atomic" and higher level components (such as load modules, data elements, and methods) that may be variously aggregated together to form control methods for electronic commerce applications, commercial electronic agreements, and data security arrangements."

- "VDE provides a secure operating environment employing VDE foundation elements along with secure independently deliverable VDE components that enable electronic commerce models and relationships to develop."

- "VDE specifically supports the unfolding of distribution models in which content providers, over time, can expressly agree to, or allow, subsequent content providers and/or users to participate in shaping the control information for, and consequences of, use of electronic content and/or appliances. A very broad range of the functional attributes important for supporting simple to very complex electronic commerce and data security activities are supported by capabilities of the present invention. As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements."

- "VDE supports a general purpose foundation for secure transaction management, including usage control, auditing, reporting, and/or payment. This general purpose foundation is called "VDE Functions" ("VDEFs"). VDE also supports a collection of "atomic" application elements (e.g., load modules) that can be selectively aggregated together to form various VDEF capabilities called control methods and which serve as VDEF applications and operating system functions."

- "VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes)."

- "the end-to-end nature of VDE applications, in which content 108 flows in one direction, generating reports and bills 118 in the other, makes it possible to perform "back-end" consistency checks."

- "VDE can protect a collection of rights belonging to various parties having in rights in, or to, electronic information. This information may be at one location or dispersed across (and/or

moving between) multiple locations. The information may pass through a "chain" of distributors and a "chain" of users. Usage information may also be reported through one or more "chains" of parties. In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed."

- "VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. These parties may include content providers, electronic hardware manufacturers, financial service providers, or electronic "infrastructure" companies such as cable or telecommunications companies."

- "A rights application under VDE is made up of special purpose pieces, each of which can correspond to one or more basic electronic processes needed for a rights protection environment. These processes can be combined together like building blocks to create electronic agreements that can protect the rights, and may enforce fulfillment of the obligations, of electronic information users and providers. One or more providers of electronic information can easily combine selected building blocks to create a rights application that is unique to a specific content distribution model. A group of these pieces can represent the capabilities needed to fulfill the agreement(s) between users and providers. These pieces accommodate many requirements of electronic commerce including: the distribution of permissions to use electronic information; the persistence of the control information and sets of control information managing these permissions; configurable control set information that can be selected by users for use with such information; data security and usage auditing of electronic information; and a secure system for currency, compensation and debit management."

- "VDE allows electronic arrangements to be created involving two or more parties. These agreements can themselves comprise a collection of agreements between participants in a commercial value chain and/or a data security chain model for handling, auditing, reporting, and payment. It can provide efficient, reusable, modifiable, and consistent means for secure electronic content: distribution, usage control, usage payment, usage auditing, and usage reporting."

- "The features of VDE allow it to function as the first trusted electronic information control environment that can conform to, and support, the bulk of conventional electronic commerce and data security requirements. In particular, VDE enables the participants in a business value chain

model to create an electronic version of traditional business agreement terms and conditions and further enables these participants to shape and evolve their electronic commerce models as they believe appropriate to their business requirements."

- "VDE provides the widely varying secure control and administration capabilities required for:

- 1. Different types of electronic content,

- 2. Differing electronic content delivery schemes,

- 3. Differing electronic content usage schemes,

- 4. Different content usage platforms, and

- 5. Differing content marketing and model strategies."

- "VDE controls auditing and reporting of electronic content and/or appliance usage."

- "VDE also securely supports the payment of money owed (including money owed for content and/or appliance usage) by one or more parties to one or more other parties, in the form of electronic credit and/or currency."

- "VDE can securely manage the integration of control information provided by two or more parties. As a result, VDE can construct an electronic agreement between VDE participants that represent a "negotiation" between, the control requirements of, two or more parties and enacts terms and conditions of a resulting agreement. VDE ensures the rights of each party to an electronic agreement regarding a wide range of electronic activities related to electronic information and/or appliance usage."

- "VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed finctionality. Furthermore, VDE permits participants to develop business models not feasible with non- electronic commerce, for example, involving detailed reporting of content usage information, large numbers of distinct transactions at hitherto infeasibly low price points, "pass-along" control information that is enforced without involvement or advance knowledge of the participants, etc."

- "VDE can support "real" commerce in an electronic form, that is the progressive creation of commercial relationships that form, over time, a network of interrelated agreements representing a value chain business model. This is achieved in part by enabling content control information to

develop through the interaction of (negotiation between) securely created and independently submitted sets of content and/or appliance control information. Different sets of content and/or appliance control information can be submitted by different parties in an electronic business value chain enabled by the present invention. These parties create control information sets through the use of their respective VDE installations. Independently, securely deliverable, component based control information allows efficient interaction among control information sets supplied by different parties."

- "Employing VDE as a general purpose electronic transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. For example, VDE allows content creators to use the same VDE foundation control arrangement for both content authoring and for licensing content from other content creators for inclusion into their products or for other use. Clearinghouses, distributors, content creators, and other VDE users can all interact, both with the applications running on their VDE installations, and with each other, in an entirely consistent manner, using and reusing (largely transparently) the same distributed tools, mechanisms, and consistent user interfaces, regardless of the type of VDE activity."

- "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information."

- "VDE can further be used to enable commercially provided electronic content to be made available to users in user defined portions, rather than constraining the user to use portions of content that were "predetermined" by a content creator and/or other provider for billing purposes."

- "VDE supports a "universe wide" environment for electronic content delivery, broad dissemination, usage reporting, and usage related payment activities."

- "VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy rights. VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are

separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered."

- "VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box, " a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means."

- "VDE supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage rights of departments, users, and/or projects."

- "Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of electronic appliances and host operating systems, VDE containers, content control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce VDE control information."

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). ... Without such separation between these basic VDE capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. ... VDE modular separation of these basic

capabilities supports the programming of plural, "arbitrary" relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information."

- "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content."

- "A further feature of VDE provided by the present invention is that creators, distributors, and users of content can select from among a set of predefined methods (if available) to control container content usage and distribution functions and/or they may have the right to provide new customized methods to control at least certain usage functions (such "new" methods may be required to be certified for trustedness and interoperability to the VDE installation and/or for of a group of VDE applications)."

- "Each VDE participant in a VDE pathway of content control information may set methods for some or all of the content in a VDE container, so long as such control information does not conflict with senior control information already in place ...."

- "VDE supports commercially secure "extended" value chain electronic agreements. VDE can be configured to support the various underlying agreements between parties that comprise this extended agreement."

- "VDE agreements support evolving ("living") electronic agreement arrangements that can be modified by current and/or new participants through very simple to sophisticated "negotiations" between newly proposed content control information interacting with control information already in place ...."

- "All participants of VDE 100 have the innate ability to participate in any role."

- "any end-user may redistribute information received to other end-users."

- "Any VDE user 112 may assign the right to process information or perform services on their behalf to the extend allowed by senior control information."

- "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain

component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500."

- "An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network."

- "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed."

- "The present inventions also provide for the use of a trusted third party electronic go-between or intermediary in various forms, including the "virtual presence" of such go-between through the rules and controls it contributes for distributed governance of transactions described in the present invention, and further through the use of a distributed, go-between system operating in on-line and/or off-line modes at various user and/or go-between sites. Such a trusted third-party go-between can provide enhanced and automated functionality, features and other advantages such as, for example .... These and other features and advantages provided by the present invention ..."

- "The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". The present inventions use (and in some cases, build upon and enhances) this fundamental Virtual Distribution Environment technology to provide still additional flexibility, capabilities, features and advantages. The present invention, in its preferred embodiment, is intended to be used in combination a broad array of the features described in Ginter, et al, including any combination of the following:...."

- "parties using the Virtual Distribution Environment can participate in commerce and other transactions in accordance with a persistent set of rules they electronically define."

- "The present inventions preferred embodiment make use of a digital Virtual Distribution Environment (VDE) as a major portion of its operating foundation, providing unique, powerful capabilities instrumental to the development of secure, distributed transaction-based electronic commerce and digital content handling, distribution, processing, and usage management."

- "The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". The present inventions use (and in some cases, build upon and enhances) this fundamental Virtual Distribution Environment technology to provide still additional flexibility, capabilities, features and advantages. The present invention, in its preferred embodiment, is intended to be used in combination a broad array of the features described in Ginter, et al, including any combination of the following: ..."

- "The Present Invention Solve These and Other Problems

As discussed above, a wide variety of techniques are currently being used to provide secure, trusted confidential delivery of documents and other items. Unfortunately, none of these previously existing mechanisms provide truly trusted, virtually instantaneous delivery on a cost-effective, convenient basis and none provide rights management and auditing through persistent, secure, digital information protection.

In contrast, the present inventions provide the trustedness, confidentiality and security of a personal trusted courier on a virtually instantaneous and highly cost-effective basis. They provide techniques, systems and methods that can being to any form of electronic communications (including, but not limited to Internet and internal company electronic mail) an extremely high degree of trustedness, confidence and security approaching or exceeding that provided by a trusted personal courier. They also provide a wide variety of benefits that flow from rights management and secure chain of handling and control."

- "The present inventions make use of these persistent electronic rules to provide secure, automated, cost-effective electronic control for electronic document and other digital item handling and/or delivery, and for the electronic formation and negotiation of legal contracts and other documents."

- "By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions:

- Trustedness and security approaching or exceeding that of a personal trusted courier. ..
- Optional delayed delivery ("store and forward").
- Broadcasting to multiple parties. ...

- Trusted validation of item contents and delivery.
- Value Added Delivery and other features selectable by the sender and/or recipient.
- Provides electronic transmission trusted auditing and validating.
- Allows people to communicate quickly, securely, and confidentially.
- Communications can later be proved through reliable evidence of the communications transaction--providing non-repudiatable, certain, admissible proof that a particular communications transaction occurred.
- Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.
- Supports persistent rights and rules based document workflow management at recipient sites.
- System may operate on the Internet, on internal organization and/or corporate networks ("intranets" irrespective of whether they use or offer Internet services internally), private data networks and/or using any other form of electronic communications.
- System may operate in non-networked and/or intermittently networked environments.
- Legal contract execution can be performed in real time, with or without face to face or ear-to-ear personal interactions (such as audiovisual teleconferencing, automated electronic negotiations, or any combination of such interactions) for any number of distributed individuals and/or organizations using any mixture of interactions.
- The items delivered and/or processed may be any "object" in digital format, including, but not limited to, objects containing or representing data types such as text, images, video, linear motion pictures in digital format, sound recordings and other audio information, computer software, smart agents, multimedia, and/or objects any combination of two or more data types contained within or representing a single compound object.
- Content (executables for example) delivered with proof of delivery and/or execution or other use.
- Secure electronic containers can be delivered. The containers can maintain control, audit, receipt and other information and protection securely and persistently in association with one or more items.
- Trustedness provides non-repudiation for legal and other transactions.
- Can handle and send any digital information (for example, analog or digital information representing text, graphics, movies, animation, images, video, digital linear motion pictures,

sound and sound recordings, still images, software computer programs or program fragments, executables, data, and including multiple, independent pieces of text; sound clips, software for interpreting and presenting other elements of content, and anything else that is electronically representable).

- Provides automatic electronic mechanisms that associate transactions automatically with other transactions.
- System can automatically insert or embed a variety of visible or invisible "signatures" such as images of handwritten signatures, seals, and electronic "fingerprints" indicating who has "touched" (used or other interacted with in any monitorable manner) the item.
- System can affix visible seals on printed items such as documents for use both in encoding receipt and other receipt and/or usage related information and for establishing a visible presence and impact regarding the authenticity, and ease of checking the authenticity, of the item.
- Seals can indicate who originated, sent, received, previously received and redistributed, electronically view, and/or printed and/or otherwise used the item.
- Seals can encode digital signatures and validation information providing time, location, send and/or other information and/or providing means for item authentication and integrity check.
- Scanning and decoding of item seals can provide authenticity/integrity check of entire item(s) or part of an item (e.g., based on number of words, format, layout, image--picture and/or test--composition, etc.).
- Seals can be used to automatically associate electronic control sets for use in further item handling.
- System can hide additional information within the item using "stenanography" for later retrieval and analysis.
- Steganography can be used to encode electronic fingerprints and/or other information into an item to prevent deletion.
- Multiple steganographic storage of the same fingerprint information may be employed reflecting "more" public and "less" public modes so that a less restricted steganographic mode (different encryption algorithm, keys, and/or embedding techniques) can be used to assist easy recognition by an authorized party and a more private (confidential) mode may be readable by only a few parties (or only one party) and comprise of the less restricted mode may not affect the security of the more private mode.

- Items such as documents can be electronically, optically scanned at the sender's end--and printed out in original, printed form at the recipient's end.
- Document handlers and processors can integrate document scanning and delivery.
- Can be directly integrated into enterprise and Internet (and similar network) wide document workflow systems and applications.
- Secure, tamper-resistant electronic appliance, which may employ VDE SPUs, used to handle items at both sender and recipient ends.
- "Original" item(s) can automatically be destroyed at the sender's end and reconstituted at the recipient's end to prevent two originals from existing simultaneously.
- Secure, non-repudiable authentication of the identification of a recipient before delivery using any number of different authentication techniques including but not limited to biometric techniques (such as palm print scan, signature scan, voice scan, retina scan, iris scan, biometric fingerprint and/or handprint scan, and/or face profile) and/or presentation of a secure identity "token."
- Non-repudiation provided through secure authentication used to condition events (e.g., a signature is affixed onto a document only if the system securely authenticates the sender and her intention to agree to its contents).
- Variety of return receipt options including but not limited to a receipt indicating who opened a document, when, where, and the disposition of the document (stored, redistributed, copied, etc.). These receipts can later be used in legal proceedings and/or other contexts to prove item delivery, receipt and/or knowledge.
- Audit, receipt, and other information can be delivered independently from item delivery, and become securely associated with an item within a protected processing environment.
- Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be "destroyed" after a certain elapse of time or real time or after a certain number of handlings, etc.)
- Persistent secure electronic controls can continue to supervise item workflow even after it has been received and "read."
- Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility.

- Secure controls can be used in conjunction with digital electronic certificates certifying as to identity, class (age, organization membership, jurisdiction, etc.) of the sender and/or receiver and/or user of communicated information.
- Efficiently handles payment and electronic addressing arrangements through use of support and administrative services such as a Distributed Commerce Utility as more fully described in the copending Shear, et al. application.
- Compatible with use of smart cards, including, for example, VDE enabled smart cards, for secure personal identification and/or for payment.
- Transactions may be one or more component transactions of any distributed chain of handling and control process including Electronic Data Interchange (EDI) system, electronic trading system, document workflow sequence, and banking and other financial communication sequences, etc."

"All of these various coordination steps can be performed nearly simultaneously, efficiently, rapidly and with an extremely high degree of trustedness based on the user of electronic containers 302 and the secure communications, authentication, notarization and archiving techniques provided in accordance with the present inventions." The asserted claims also are invalid for violating the enablement and written description requirements to the extent that they are construed to recite subject matter that was not enabled by the application from which they issued, and/or not disclosed (e.g., the claims recite an element that was not disclosed in the written description, recite an element more broadly than was disclosed by the written description, recite subject matter for which there were no "blaze marks" in the written description pointing to such subject matter, combine elements from different embodiments that were not so combined in the written description, etc.) in that application. For example, at least the following bold-faced claim language was not so enabled and/or disclosed, at least not as the claims apparently are being "construed" by InterTrust to attempt to support its untenable infringement allegations:

'193

1) A method comprising:

a) receiving a digital file including music;

b) **storing said digital file in a first secure memory of a first device**;

c) **storing information associated with said digital file in a secure database stored on said first device, said information including at least one budget control and at least one copy control, said at least one budget control including a budget specifying the number of copies**

which can be made of said digital file; and said at least one copy control controlling the copies made of said digital file;

d) **determining whether said digital file may be copied and stored on a second device based on at least said copy control;**

e) **if said copy control allows at least a portion of said digital file to be copied and stored on a second device,**

f) **copying at least a portion of said digital file;**

g) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

h) storing said digital file in said memory of said second device; and

i) including playing said music through said audio output.

2) A method as in claim 1, further comprising:

a) at a time substantially contemporaneous with said transferring step, recording in said first device information indicating that said transfer has occurred.

3) A method as in claim 2, in which:

a) **said information indicating that said transfer has occurred includes an encumbrance on said budget.**

4) A method as in claim 3, in which:

a) **said encumbrance operates to reduce the number of copies of said digital file authorized by said budget.**

11) A method comprising:

a) receiving a digital file;

b) **storing said digital file in a first secure memory of a first device;**

c) **storing information associated with said digital file in a secure database stored on said first device, said information including a first control;**

d) **determining whether said digital file may be copied and stored on a second device based on said first control, said determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said second**

device, said determination based at least in part on the features present at the device to which said copied file is to be transferred;

e) if said first control allows at least a portion of said digital file to be copied and stored on a second device,

f) copying at least a portion of said digital file;

g) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

h) storing said digital file in said memory of said second device; and

i) rendering said digital file through said output.

15) A method comprising:

a) receiving a digital file;

b) an authentication step comprising:

c) accessing at least one identifier associated with a first device or with a user of said first device; and

d) **determining whether said identifier is associated with a device and/or user authorized to store said digital file;**

e) **storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;**

f) **storing information associated with said digital file in a secure database stored on said first device, said information including at least one control;**

g) **determining whether said digital file may be copied and stored on a second device based on said at least one control;**

h) **if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,**

i) **copying at least a portion of said digital file;**

j) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

k) storing said digital file in said memory of said second device; and

l) rendering said digital file through said output.

19) A method comprising:

a) receiving a digital file at a first device;

b) **establishing communication between said first device and a clearinghouse located at a location remote from said first device**;

c) **said first device obtaining authorization information including a key from said clearinghouse**;

d) **said first device using said authorization information to gain access to or make at least one use of said first digital file, including using said key to decrypt at least a portion of said first digital file**; and

e) **receiving a first control from said clearinghouse at said first device**;

f) storing said first digital file in a memory of said first device;

g) **using said first control to determine whether said first digital file may be copied and stored on a second device**;

h) **if said first control allows at least a portion of said first digital file to be copied and stored on a second device**,

i) **copying at least a portion of said first digital file**;

j) transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;

k) storing said first digital file portion in said memory of said second device; and

l) rendering said first digital file portion through said output.

'683

2. A system including:

a first apparatus including,

user controls,

a communications port,

a processor,

a memory storing:

a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;

a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule, the first secure container rule having been received from a third apparatus different from said second apparatus; and

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said **protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

28. A system including;

a first apparatus including;

user controls,

a communications port,

a processor,

a memory containing a first **rule,**

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a **protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus**, said **protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item**; and

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

a second apparatus including:

user controls,

a communications port,

a processor,

a memory containing a second **rule**,

hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;

a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said **protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;**

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and

an electronic intermediary, said intermediary including a user rights authority clearinghouse.

29. A system as in claim 28, said **user rights authority clearinghouse operatively connected to make rights available to users.**

PLR 3-4 Production

Each reference identified pursuant to PLR 3-3(a) but not in the prosecution history, and the documents referenced in PLR 3-4 that are sufficient to show the operation of the accused features of the products specifically identified in InterTrust's PLR 3-1 Statements of October 29 and November 5, 2001, and "Addendum" dated March 12, 2002, has been or is being produced, or is otherwise available for inspection and copying.

Dated: August 16, 2002

By: _____

WILLIAM L. ANTHONY, State Bar No. 106908
ERIC L. WESENBERG, State Bar No. 139696

HEIDI L. KEEFE, State Bar No. 178960
MARK R. WEINSTEIN, State Bar No. 193043
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
MICROSOFT CORPORATION

Of Counsel:

T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE BY MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 121 S.W. Salmon St., Portland, Oregon 97204

On August 16, 2002, I served:

MICROSOFT'S PRELIMINARY INVALIDITY CONTENTIONS REGARDING U.S. PATENTS 6,253,193 & 6,185,683 PURSUANT TO PLR 3-3, 3-4

by e-mail and by placing true copies of these papers in each of separate envelopes addressed to:

Michael Page, Esq. KEKER & VAN NEST, LLP 710 Sansome Street San Francisco, CA 94111 mhp@kvn.com	Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 steven.morrissett@finnegan.com
	Stephen E. Taylor, Esq. Taylor &Co. Law Offices 1050 Marina Village Parkway Suite 101 Alameda, CA 94501 staylor@tcolaw.com

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Portland, Oregon.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 16, 2002, at Portland, Oregon.

_____

(SIGNATURE)

_____

(PRINT NAME)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

MICROSOFT PLR 3-3(c) CHARTS

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
2. A system including:		Reference is made to (1) each Stefik reference cited in the asserted InterTrust patents, and to USP 5,715,403; (2) all related methods practiced at Xerox PARC and/or ContentGuard prior to InterTrust's alleged priority date	Reference is made to Proceedings, Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project, v. 1 no. 1 (Jan 1994) ("CNI/IMA 94"), and its 1993 proceedings in Cambridge, MA	Reference is made to "Copyright Protection for Electronic Publishing over Computer Networks," A.K. Choudhury, N.F. Maxemchuk, S. Paul, H.G. Sculzrinne.	Reference is made to Tygar & Yee, "Strongbox: A System for Self-Securing Programs" in CMU Computer Science: A 25th Anniversary Commemorative, R. Rashid, ed. (ACM Press 1991) ("SB"); "Cryptography: It's Not Just for E-mail Anymore," (Tech. Report CMU-CS-93-107, Carnegie Mellon Unic. March 1993) ("ES"); and/or "Dyad: A System for Using Physically Secure Coprocessors." (Carnegie Mellon Univ., CMU-CS-91-140R, May 4, 1991) (see also CNI/IMA 94). Dyad refers to and supplements the Strongbox and ES references; SB comprises a loosely coupled network of machines with different security levels, using key exchange, secure processors and memory, authentication and capabilities, finger printing, and verified boot
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	E.g., a computer. See, e.g., USP 5,715,403; USP 5,634,012.	A computer. See, e.g., R. J. Linn, "Copyright and Information Services in the Context of the National Research and Education Network" and references to it; Robert E. Kahn, "Deposit, Registration and Recordation in an Electronic Copyright Management System" ("Kahn"); J.D. Tygar and Bennet Yee, "Dyad: A System for Using Physically Secure Coprocessors" ("Dyad"); see also, e.g., Cupid, KALA, and Griswold articles	First apparatus could be any "client" or user computer, or any document or copyright server. See e.g. Figs. 1 & 2.	ES: any first user's "apparatus," e.g. a computer); electric postage meter (EPM); printer; Post Office computer; SB: any first "apparatus"
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	"apparatus" has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	one or more comm. ports
(3) a processor,	Consumer's computer, as shown	See 2(a)	See 2(a)	See 2(a)	a processor

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
	in WMRM SDK				
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	and a memory storing:
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	"secure container" is indefinite, but as used by InterTrust in its 3-1 Statement would include the digital works described in Stefik, and/or (or such as) digital certificates or authorizations. Systems or components (including digital works) may be object-oriented.[1]	"secure container" and "item" are indefinite, but as used by InterTrust in its 3-1 Statement appear to include, for example, any file having any aspect of "security." Such an "item" may be a message or literary or instructional text, for example. Part or all of such "items" may be encrypted; it would also be obvious that one could do so. Note also that in Linn, Kala, Dyad et al., systems and/or components may be object-oriented. By InterTrust's allegations, additional examples of "secure containers" in e.g. Dyad could be the secure coprocessor and/or its associated software, a contract or contract template, a partly or wholly encrypted program, electronic currency, or smart cards.	By InterTrust's construction, any file received from any 2nd apparatus (e.g. floppy or download, e.g. from the "document server") any part of which is "encrypted"	ES: stamp (currency) is received from provider (EPM) and stored on user apparatus SB: any self-securing program(s) or other encrypted information
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	"Rule" is indefinite, but as used by InterTrust in its 3-1 Statement this element would include certificates and other digital works that move between repositories subject to usage rights (and which can come from a 3d source)	numerous so-called "rules" may be received from any third apparatus, such as right to render or copy. See, e.g., Linn, Kahn (EBR, terms and conditions on use, usage restrictions and/or payment requirements), Dyad (bindings, 3rd party instructions, contracts, contract bindings, additional contracts, secure coprocessor-supported requirements, other secure coprocessors and/or associated hardware or software, and upgrades or further upgrades)	satisfying copyright server's authentication request(s) (e.g. through permission, signature, authentication, access controls (persona, anonymous, user)), name and password, access control lists, capabilities, shared secrets, challenge-response, encryption (public key and/or symmetrical), key certificate techniques, Kerberos	ES: any currency "rule" received from 3d apparatus (e.g., permission from root, or passphrase from keyboard or other apparatus); rights portion from EPM SB: any partly or wholly encrypted information from any White Pages server, and/or fingerprinted data or program files
(5) hardware or software used for receiving and opening secure	Windows Media Player and Windows Media Rights	system hardware or software	system hardware or software	client and server hardware or software	ES: EPM and associated hardware or software

[1] It was obvious to use any known techniques as in e.g. Smalltalk, Bento and/or OLE/COM in connection with disclosures of Stefik, CNI/IMA 94, Choudhury/Maxemchuk, Tygar/Yee, Blaze, etc. See, for example, W. LaLonde, J. Pugh, Inside Smalltalk (Prentice Hall 1990); Harris et al., Apple Bento, Specification v 1.0d5 (July 1993); Peter Coad, "Object Oriented Patterns" (Comm. of the ACM, Sept. 1992); OLE 2 Programmers Reference vol. 1 (Microsoft Press 1994). For example, using the observer design pattern or model view controller or broadcast pattern, objects can initiate notifications regarding embedded objects, e.g., objects may be saved to secure data stream and transferred to other controls. Another example is the COM Service Control Manager.

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Manager				SB: e.g. SB, Mach, Camelot, secure processor
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	e.g. protected repositories, certificates, usage rights, and associated systems and software	describes numerous examples of what InterTrust appears to consider "protected processing environments" where "rules" are applied	1st and 2nd "rules" consist of any 2 valid "rules" referenced above; alleged "PPE" includes protected client and server processes	ES: 1st and 2nd "rules" consist of any two valid "rules" specified above; "PPE" as alleged would include the application and OS processes for protecting operation of the system SB: "secure" loader (second server), and/or any user-supplied access-control/authorization system (167)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	hardware or software used for transmission	hardware or software used for transmission	system hardware or software (see e.g. Figs. 1-2)	ES: any hardware or software employed in transmitting currency SB: see 2(a)(4)(i); any system hardware or software employed in transmission
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	any user apparatus (e.g. P.C.) with: See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	a communications port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	client or server apparatus	a processor, and
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	See 2(a)	See 2(a)	client or server apparatus	a memory containing a "first rule"
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or	See 2(a)(5)	See 2(a)(5)	client or server apparatus	ES: EPM and associated hardware and software SB: See 2(a)(5)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
being associated with each of said secure containers;	rules via Windows Media Player and Windows Media Rights Manager.				
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	See 2(a)(6)	process environment protected from tampering; "rules" applied to govern access or use of file contents	protected client and server processes apply "rules" according to InterTrust	see 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)
(b) a second apparatus including:	2nd consumer's computer	See 2(a)	2nd client or server apparatus	2nd user apparatus	2nd user apparatus
(1) user controls,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(2) a communications port,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(3) a processor,	2nd consumer's computer	See 2(a)	See 28(b)	2nd user apparatus	2nd user apparatus
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	Memory in a repository or other user apparatus; usage rights and/or security levels supply "rules"	memory in 2nd apparatus contains "second rule" according to InterTrust	memory in 2nd apparatus contains "second rule" according to InterTrust	2nd user apparatus
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 28(a)(5)	see 28(a)(5)	2nd user's apparatus; "secure container rule or rules" applied via e.g. OS (e.g. Mach, Unix) and/or file systems like CFS or Andrew. See also 28(a)(5)	2nd user's apparatus; "secure container rule or rules" applied via e.g. OS (e.g. Mach, Unix) and/or file systems like CFS or Andrew. See also 28(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media	see 28(a)(6)	see 28(a)(6)	see 28(a)(6)	see 28(a)(6)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	CNI/IMA 94	Choudhury/Maxemchuk et al.	Tygar/Yee
processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Rights Manager; processing environment applies multiple rules in combination				
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 28(a)(7)	see 28(a)(7)	see 28(a)(7)	see 28(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	Credit server or any (other) "intermediary" repositories for user or usage rights or capabilities	Linn - copyright server or other "intermediary"/"rights-issuer" connected to other users of system; Kahn – RMS, RRS, and/or repositories; Dyad – any machine or system (such as a distributor or contractor) serving alleged "clearinghouse" function	copyright server	ES: local P.O. (or EPM with multiple users) SB: White Pages server
29. A system as in claim 28,					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	28(c) above, "operatively connected" to user(s)	28(c) above, "operatively connected" to user(s)	28(c) above, "operatively connected" to user(s)	ES: local or other P.O. (or EPM with multiple users) "operatively connected" to make rights available to users SB: White Pages server

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) - continued

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
2. A system including:		Reference is made to B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed Systems," Proceedings of the 13th Int'l Conf. on Distributed Computing Systems, May 1993; see also www.isi.edu/people/bcn/publications.html	Reference is made to D. W. Davies, W. L. Price, Security for Computer Networks (John Wiley & Sons 1989) See, for example, Chapter 6, "Key Management"; see also the description of ATMs, EFT & POS systems (e.g., pp. 297-339); reference is also made to the public knowledge, use, and sale of such systems in the U.S. prior to 2/13/94; see also S. Muftic, Security Mechanisms for Computer Networks (Halstead Press, a div. of John Wiley & Sons, 1984) re authentication cards	Reference is made to David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. of the ACM, vol. 28 no. 10, Oct. 1985; see also "Wallet Databases with Observers," Advances in Cryptology-Proceedings of Crypto '92 (pp. 89-105; "Achieving Electronic Privacy," (Scientific American 1992); www.chaum.com/articles/list_of_articles.htm	Reference is made to each of RSA Data Security Conference 1/12-14/94 (re Telescript, RSA, General Magic); USP 5,603,031; USP 6,016,393; and White, J.E., Telescript Technology: The Foundation for the Electronic Marketplace (1994). On information and belief, Telescript was also used in AT&T PersonaLink before 2/13/95.	Reference is made to each of Custer, Inside NT (Microsoft Press 1993) and NT software, including NT security levels and/or NT in combination with Kerberos or other certificate, signature or other encryption methods (e.g., Kerberos API routed through NT security subsystem). See e.g. Custer at 26-31, 329-30.	This claim as asserted is also anticipated by a simple Bell-LaPadula model, widely known in the U.S. before 2/13/94 -- see, e.g., discussion in Castano et al., Database Security (Addison Wesley 1994)
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	e.g. client c in Fig. 3	any computer in a network, e.g. terminal 2 in Figure 6.3, or an ATM machine or bank computer (e.g. in shared ATM systems)	any first computer, e.g. a personal card computer	a first computer having	a first PC (client or server)	Apparatus 1 could also be a filesystem computer
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	has user controls	user controls	has user controls	has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a comm port	a comm port	a comm port	a comm port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a processor	a processor	a processor	a processor

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	memory stores:	and a memory	and a memory	and a memory	and a memory
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	so-called "secure container" as alleged by InterTrust would cover Kerberos tickets which may be received from a server, e.g. for a read capability. Alternatively, any partly encrypted file.	encrypted files, messages, session keys and terminal keys; ATM card or wholly or partly encrypted instructions or data received from bank computer (e.g., balance)	One or more enabling credentials or "container" thereof	a first agent (object), or associated file, encrypted in whole or part, received from a 2d "apparatus."	File with any "item" "at least in part encrypted" received from a second "apparatus" – e.g., a cryptographically signed and/or sealed or otherwise at least partly encrypted file received from another computer	a second apparatus operating at a particular security level may develop information (an object) classified at a particular security level, and store it at apparatus 1
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	so-called "rule" received from e.g. server or end server, or knowledge about the authorization received from another source; capabilities may be revocable and have expiration times; access control lists support compound principal identifiers	"rule" of any transaction, or PIN or watermark and/or user ID from card; "rights portion" of data sent from key distribution server	applying any "rule" obtained from a "shop" or "rule" for exposing credit info	a permit from a 3d apparatus (e.g. associated with a 2d agent meeting a 1st)	InterTrust's 3-1 Statement uses "rule" in so general a sense that it could be any password, key, ticket, permission, clearance, right, capability, or access control used in NT (see (6) below)	when a third apparatus seeks access to stored object, it must provide security level information (e.g. a security label)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	passim; possible "rules" include for-use-by-group, accept-once, quota, authorized, limit-restriction	system hardware or software for opening files, messages, deciphering session keys; ATM receives cards having keys or other "governed" data; receives data from bank computers	system hardware or software, e.g. to process credentials	system hardware or software, e.g. engine	system hardware or software	system hardware or software (e.g., Apparatus 1 applies BLP rules, which determines whether the third apparatus is granted access or not. Permissions include but are not limited to write, read, copy, execute).
(6) a protected processing environment at least in part protecting information contained in said protected	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights	"rules" as asserted by InterTrust may be any of multiple (e.g.	second "rule" could be, e.g., balance information, account limits, or any other	processing has safeguards; "rules" allow electronic commerce of varying	processing has safeguards; "rules" as InterTrust alleges the term would cover permits	"1st and 2nd rules" as alleged by InterTrust could consist of any 1 or more of	processing has safeguards; see, e.g. (5) re BLP rules. It would also be obvious to

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	cascaded) proxies; any accounting rules; any policy programming steps; and any underlying access controls or other authorization or authentication. See also Kerberos	contractual rule or access requirement; use of session key and terminal key to decipher a file/message, see e.g. Figure 6.3; using the keys to authenticate the terminals; applying authentication and decipherment to open files/messages	characteristics	and intersections as well as meeting results, in service of policies or any transaction calculus	the features which protect information in NT, including access controls, security subsystem, security reference monitor and passwords, login, Kerberos, enforces security policies, guards operating system resources, and performs run-time object protection and auditing; see also data shielding and integrity functions, e.g. in communications, computing, and databases.	use any of the cumulative protections described in the accompanying document under Suggestions to combine and motivations to combine.
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	hardware or software employed in transmitting tickets	any hardware and software use to transmit files/messages between terminals; e.g. ATMs and the rest of the associated banking system	personal card computer has transmission capabilities	hardware or software is used for transmission	any hardware or software employed in transmitting files or tickets	hardware or software is used for transmission
28. A system including:							
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)
(4) a memory containing a first rule,	Memory is in the consumer's computer,	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)	See 2(a)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
	first rule is a right received as part of a signed license (WMRM SDK, Step9)						
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)	See 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
(b) a second apparatus including:	2nd consumer's computer	any 2d computer	any 2d computer (e.g., of terminals 1, 2); a 2d ATM or bank computer	any 2d card or other device	any 2d computer	Any second computer, e.g. server or client computer running NT	any second user's computer
(1) user controls,	2nd consumer's computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(2) a communications port,	2nd consumer's computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(3) a processor,	2nd consumer's computer	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)	See 28(b)
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)	See 2(a)(4)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)	See 2(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
			USENIX Conference Proceedings, 1994)	Discretionary Security Model for Object-oriented Databases" in G.G. Gable and W.J. Caelli (eds.), IT Security: The Need for International Cooperation, 345-357 (Elsevier 1992); Olivier, M., et al, "A Taxonomy for Secure Object-Oriented Databases," ACM Transactions on Database Systems, Vol. 19, No. 1, 1994; Olivier, M., "Secure Object Oriented Databases," Doctoral Thesis, December 1991, Rand Afrikaans University.	
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop[2]	any user apparatus (e.g., a host machine or client PC)	any computer in the distributed network	First apparatus is recipient's (Bob) computer.
(1) user controls,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	any computer in the distributed network	User controls of recipient computer.
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	any computer in the distributed network	Communications ports of recipient computer.
(3) a processor,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	Any computer in the distributed network	Processor of recipient computer.
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	e.g., a host machine or client PC	Any computer in the distributed network	Memory of recipient computer.
(i) a first secure containe~~Secontaining~~ a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	ainer (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	Secure/ Encrypted copy of Printjob, or Printjob Order, or content file received by Printshop from Orgination Server, Reference Server or Gatekeeper Server, having been packaged directly by or referenced (via subdocument fields within a Printjob) by the Publisher's CUPID Client.	Scenario 1 – CFS files are received from other accounts or users or by download or from floppy (e.g., content providers) Scenario 2 – any "secure" file received from sender with credential saved in another group's directory	SOODB objects could be "secure containers" as alleged by InterTrust; "governed item" may be internal data type or external by reference. Object is instantiated from remote system where it persists.	"First secure container" is transmission (datastream or file) sent from sender Alice's computer (the "second apparatus") to recipient Bob's computer. The transmission includes a message (the "governed item") sent by Alice to Bob, which is encrypted with the (shared secret) session key K_{AB}.

[2] The CUPID Architecture defines two kinds of Servers: *Origination Servers* and *Notification Servers*. These terms refer both to the software (in UNIX terms, the daemons) that provides the specified services and to the computers upon which this software is running. A single computer may operate as both an Origination Server and a Notification Server. CUPID allows Printshop systems to be organized in a variety of ways. A single program, for example, might perform all the Printshop's CUPID Client functions and also act as the printer server. Alternatively, several programs running on several computers might act as specialized CUPID Clients, communicating with a printer server running on yet another host.

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Neuman	ATMs and other examples in Davies & Price	Chaum	Telescript	NT	Bell-LaPadula
use of a governed item;							
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)	See 2(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	e.g. group server, end server, authorization server, or any remote server	key distribution center; bank "clearinghouse"	credential "clearinghouse"	any server or other machine playing "intermediate" role with "clearinghouse" function, e.g. with permits or keys	NT server in any "clearinghouse" role, e.g. admin or host; see also Kerberos	server in any "clearinghouse" role
29. A system as in claim 28,							
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)	system of 28(c)

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) - continued

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
2. A system including:		"CUPID" is described in e.g. "Protocols and Services (Version 1): An Architectural Overview" (November 1992) (CUPID Architecture Subcommittee); see also CNI/IMA 94	Reference is made to each of Blaze, "A Cryptographic File System for Unix" (First ACM Conference on Communications and Security, 1993) (and preprint); "Key Management in an Encrypting File System" (Usenix 1994); and (with John Ioannidis) "The Architecture and Implementation of Network – Layer Security Under Unix" (Proceedings of 1994 Winter	Reference is made to ORION/ITASCA and Thor secure object oriented database systems, and to the work of Martin S. Olivier in the development of SECDB, 1990-1995, at Rand Afrikaans University, South Africa. See Olivier, M., et al, "Building a Secure Database using Self-Protecting Objects," Computers & Security, Vol. 11, No. 3, 1992; Olivier, M., et al, "DISCO: A	Reference is made to J. Kohl, C. Neuman, RFC 1510, "The Kerberos Network Authentication Service (V5)"; see also descriptions of, references to and suggested combinations with Kerberos in, e.g., Davies, Neuman, Custer; see also, generally, MIT's Project Athena and secure authenticated e-mail, e.g. RFCs 1154-55

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	**Scenario 1:** Contained within a Printjob, or Printjob Order are Tasks, Operation Specifications and Pre-requisite Task Lists, each contains rules, tasks, or instructions that must be followed in order to reproduce the content file.[3] **Scenario 2:** The Printshop Client, Notification Server, or any Agents running on the Printshop Server, can access and	"rule" as alleged by InterTrust could be any of: - key received from an apparatus other than the apparatus the file came from (e.g., from root or an admin account) - smart card key(s) rcvd from smart card; - passphrase rcvd from keyboard and/or other input apparatuses	Secure container "rule" is received from third system where the class for the remote object is persisted. "Rule" implements some control over access to object, such as multi-level security or method authorization	"First secure container rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration (TD)) in the recipient ticket originating from the Kerberos server (aka, key distribution center or KDC), and forwarded to the recipient computer (first apparatus) from the sender computer (second apparatus). The recipient ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session

[3] Anatomy of a Printjob, including Printjob Order:

Printjob Header ***(which includes)***
Publisher ID;
Date and time submitted;
Job Name, used for Publisher identification purposes, not necessarily the same as the Document title;
Job Limits (optional), used to extend or reduce the default Printjob retention period on the Origination Server;
Security Keys (if and as required);
General free-text comments, intended to be seen by all Parties working on this Printjob.
[Subdocument File(s)]
Status* (includes Status of all Printjob elements)
Message Queue*
..... and 1 or more Printjob Order(s)
Printjob Order Header ***(which includes)***
Printshop ID;
Order Name (used for Publisher identification purposes);
Scheduling, priority, and/or deadline information;
Authorization codes, if any (i.e., authorization codes defined and known by the Publisher and the Printshop *outside* of CUPID, by virtue of separate contractual or other arrangements); and
General free-text comments (intended to be seen by all Parties working on this Order).
[Complete Document]
Task(s)
Operation
[Object]
[Opspecs]
[Agent]
[Prerequisite Task List]

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		download their specific tasks from the Origination Server Message Queue. These messages contain instructions that must be followed in order to reproduce the content file. **Scenario 3:** Cupid Agents may be used to govern aspects of access on use. Agents may be employed by Publishers, Printshops, or other Agents	Also in Scenario 2 – verifying credentials of sender		key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) the sender's message (governed item) at the recipient computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	The Printshop CUPID Client is responsible for receiving content files, from any source, and messages from the Origination Server Message Queue.[4]	associated networked hardware and software	SOODB process and/or object methods	Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open the sender's message on the recipient computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	The UNIX Server running at the Printshop protected from physical access or by UserID & Password. Access to content can be protected by predetermined keys stored in the Printjob Header. The Printshop CUPID Client accesses and renders the content. Caching of text, images, or other information at locations other than the Origination Server may be invisible to Clients and complies with CUPID's security provisions. The CUPID Client also ensures that any tasks or instructions are carried out according to the Message Queue,	any two valid "rules" referenced above; or 2d rule could also be logon, or Unix permission (user/group/world, read/write/execute); "PPE" may include CFS and/or Unix processes for protecting operation of system; in scenario 2, whether sender can write to designated file	the trusted architecture implementing the SOODB framework. "Second rule" as InterTrust would have it can include any identification/authorization	"Second secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use of the session key to access (decrypt) the sender's message. "PPE" is the Kerberos protocol software on the recipient computer.

[4] In CUPID, the Message Queue may reside on the Origination Server for that Printjob, and accumulate Messages related to the Printjob that are targeted for the Publisher, the Printshop, and any Agents referenced by the Printjob. A Client connecting to a Server may request the accumulated messages for the appropriate Publisher, Printshop, or Agent. [Publishers, Printshops, and Agents may be notified via electronic mail [secured by encryption or obvious to do so] that one or more CUPID messages are waiting.]

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		Pre-requisite Task List, or Tasks contained in the Printjob Order.[5]			
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	CUPID Client can either communicate directly with printer devices, or can communicate with Printer Servers for spooling and queuing of work. Subdocument Files, may be defined to be (optionally) pointers to Subdocuments, rather than the actual contents of the Subdocuments. These pointers might refer to files outside of CUPID, and may include keys or other access-control information	any hardware or software employed in transmitting files	any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Recipient computer's network card and networking protocol software.
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	any user apparatus (e.g. host machine or client P.C.)	Any computer in the distributed network	First apparatus is sender's (Alice) computer.
(1) user controls,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	User controls of sender computer.
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	Communications ports of sender computer.
(3) a processor,	Consumer's computer, as shown in WMRM SDK	UNIX Server running at a Printshop	See 2(a)	Any computer in the distributed network	Processor of sender computer.
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	UNIX Server running at a Printshop	any of: -any key or permission in memory; -smart card key(s) rcvd from	Memory of a computer in the distributed network, storing the caller's capability (i.e. non-forgeable token) for example	Memory of recipient computer. "First secure container rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration

[5] CUPID provides inter alia: (a) the network delivery of print-ready electronic documents; (b) the authorization of *who* is to print or distribute finished documents; (c) the communication of information as to *how* the document are to be printed and distributed, including steps of proofing and estimating; (d) the support of business functions, such as payment for printing services and specification and collection of royalties or other fees; (e) support for security; (f) conversion of document formats; and (g) CUPID protocols and services that support these functions.

The CUPID architecture further comprises/features:

- Internet-based utility that provides services to enable distributed printing;
- Protocol to send document over network, with job instructions and status information;
- Initial distributed services include: access control; authentication; encryption/decryption; images text conversion; routing; assembly; job status and resource tracking;
- Pointers to remote stored documents; end-user desktop assembly of custom documents; print-time merge of component materials; print-time final edit; etc.

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
			smartcard; -passphrase rcvd from keyboard or other input apparatus; -or other access limitations (such as credentials or logon), or managed resources (such as budgeted CPU time or memory)		(TD)) in the sender ticket returned from the Kerberos server (aka, key distribution center or KDC) in response to sender computer's ticket request. Sender ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) a response message (governed item) from the recipient computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	Printshop CUPID Client is responsible for receiving content files from any source, and messages from the Origination Server Message Queue.	user can use hardware or software to receive and "open" wholly or partially encrypted files	The above computer and/or associated processes. SOODB objects could be "secure containers" as alleged by InterTrust. "Governed item" may be internal data type or external by reference	"Secure container" is transmission (datastream or file) sent from recipient computer (the "second apparatus") to sender computer. The transmission includes a response message (the "governed item") sent by Bob to Alice, which is encrypted with the (shared secret) session key K_{AB}. Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open Bob's message on the sender computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	UNIX Server running at the Printshop is protected from physical access and by UserID & Password. Access to content can be protected by predetermined keys stored in the Printjob Header. CUPID Client ensures that tasks and instructions are carried out according to the	As construed by InterTrust, "1st rule" and "a secure container rule" could be any two valid "rules" referenced above; "PPE" includes file and operating system processes for protecting system operation	SOODB process and/or object methods in the trusted computing base. "Secure container rule" is received from third system where the class for the remote object is persisted. "Rule" implements some control over access to object, such as multi-level security or method authorization	"secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
		Message Queue, Pre-requisite Task List, and/or Tasks contained in the Printjob Order.			of the session key to access (decrypt) Bob's message. "PPE" is the Kerberos protocol software on the recipient computer
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	CUPID Client can communicate with Printer Servers, displays or printer devices	any hardware or software employed in transmitting wholly or partly encrypted files	Any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Sender computer's network card and networking protocol software.
(b) a second apparatus including:	2nd consumer's computer	2nd apparatus, e.g. 2nd Unix Server running at a Printshop	2nd user's apparatus	The trusted architecture implementing the SOODB framework. "Second rule" is subject identification/authorization	First apparatus is recipient's (Bob) computer.
(1) user controls,	2nd consumer's computer	2nd apparatus	2nd user apparatus	2nd apparatus	User controls of recipient computer.
(2) a communications port,	2nd consumer's computer	2nd apparatus	2nd user apparatus	2nd apparatus	Communications port of recipient computer.
(3) a processor,	2nd consumer's computer	2nd apparatus	2nd user apparatus	2nd apparatus	Processor of recipient computer.
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	memory in 2nd apparatus contains "second rule" according to InterTrust	memory in 2nd apparatus contains "second rule" according to InterTrust	memory in 2nd apparatus contains "second rule" – a classification level of the class for example	Memory of recipient computer. "Second rule" is any of four values (sender and recipient IDs, a time stamp (TS), a time duration (TD)) in the recipient ticket originating from the Kerberos server (aka, key distribution center or KDC), and forwarded by sender computer to recipient computer. Recipient ticket includes: sender and recipient IDs, a time stamp (TS), a time duration (TD), and the session key K_{AB}. The IDs, TS and TD together govern use of the session key to access (decrypt) a message (governed item) from the sender computer. For example, Kerberos protocol limits use of the session key to the time period specified by TS, TD, and limits the message exchange to the principals specified by IDs.
(5) hardware or software used for receiving and opening secure containers, said secure	2nd consumer's computer receives Windows Media file (secure container) via	second Printshop CUPID Client	same as (a)(5) for 2nd apparatus	2nd apparatus and/or associated	"Secure container" is transmission

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	running on the second Unix Server is responsible for receiving a) content files from another CUPID Client, and b) messages from the Origination Server Message Queue		processes.	(datastream or file) sent from sender computer to recipient computer. The transmission includes a message (the "governed item") sent by Alice to Bob, which is encrypted with the (shared secret) session key K_{AB}. Network adapter, networking protocol software, Kerberos protocol software or hardware, and decryption software (e.g., DES decryptor) are used to receive and open Alice's message on the recipient computer.
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	see 28(a)(6)	same as (a)(6) for 2nd apparatus	SOODB process and/or object methods in the trusted computing base. "Secure container rule" is received from third system where the class for the remote object is persisted. Rule implements some control over access to object, such as multi-level security or method authorization	"Secure container rule" is any of the other three of the four values in the recipient ticket. Note that the sender and recipient IDs in the recipient ticket actually originates from the initial ticket request from the sender computer to the KDC server. All four values in the recipient ticket are applied in combination to govern use of the session key to access (decrypt) Bob's message. "PPE" is the Kerberos protocol software on the recipient computer.
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 28(a)(7)	same as (a)(7) for 2nd apparatus	Any hardware or software allowing interconnection and intercommunication in the distributed SOODB	Sender computer's network card and networking protocol software.
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	any Agent application running on said second Unix Server responsible for clearing rights, or authorizing rights, for use of content in subdocument files, such as art, images or research materials	any "intermediary" account, such as an administrative account or root, or credential server	Electronic "intermediary" is a downgrading process or other system process specifying and resolving multi-level security concurrency conflicts or resolving covert channel problems	The Kerberos key distribution center (KDC).
29. A system as in claim 28,					
said user rights authority clearinghouse	License Issuer, operatively connected to	28(c) above, "operatively	28(c) above, "operatively	system of 28(c), e.g., Downgrader	KDC is networked with sender's,

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	CUPID	Blaze	Object Oriented Database Systems	Kerberos
operatively connected to make rights available to users.	consumer's computer (WMRM SDK, Step 9)	connected" to user(s)	connected" to users	process is "operatively connected" to the SOODB as is the resolver process.	recipient's and others' computers to provide the tickets.

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust) (continued)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
2. A system including:		Reference is made to Cox, Brad J., "SUPER DISTRIBUTION AND ELECTRONIC OBJECTS - What if there is a silver bullet...and the competition gets it first?" (Dr. Dobbs Journal, Oct. 1992)), discussing e.g. Mori, Ryoichi and Masaji Kawahara, "Superdistribution: The Concept and the Architecture," Transactions of the IEICE, vol. E 73 (July, 1990). (A version of this Cox article first appeared in the Journal of Object-oriented Programming (June, 1992); see also Cox, Brad J. "There is a Silver Bullet." BYTE (October, 1990)).	Reference is made to Gary Griswold, "A Method for Protecting Copyright on Networks," in IMA/CNI 94, above, and the demo version referenced therein; see also WO93/01550	Reference is made to IBM Corp.'s "Cryptolope" system and software (hereafter "C") Reference is made to "iOpener System Description," (National Semiconductor 1993) ("iO"), and National Semiconductor's "iPower" product(s), including as publicly proposed or disclosed in combination with EPR & "VDE" ("iP")	Reference is made to Lampson, et al., Authentication in Distributed Systems, ACM 1992. See also, e.g., Authentication and Delegation with Smart Cards, M. Abadi, M. Burrows, C. Kaufman, and B. Lampson *Science of Computer Programming* **21**, 2 (Oct. 1993), pp 91-113; Authentication in the Taos Operating System (1993).
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	vendor or clearinghouse or consumer device having an S-box, e.g. an S-computer	user's computer	user's computer	any computer in the distributed network
(1) user controls,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	has user controls
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	a comm port
(3) a processor,	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	a processor
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	see 2(a)	see 2(a)	see 2(a)	and a memory
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been	Secure container (packaged Windows Media file), received by consumer's computer from	e.g. S-software, S-programs, music, &/or payment files	software envelope	C: Cryptolope iO, iP: at least partly	fields of credential received from 2d apparatus may be encrypted, e.g. identity of principle making the

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
received from a second apparatus;	"Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")			encrypted data received by user	request embodied in the "governed data item"
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	vendor et al. can supply one or more "rules" and can cancel privileges; "rules" can also be in account file information, or credit limits set or reset by sales outlets or agents. Files are also subject to access rules, authentication of user by host, etc.	central authorizing site governs aspects of use and/or access	C: "rights portion" of e.g. "license cryptolope" iO: UMS can supply "rules" (or content)	the verification information received from appliance 3 is a "rule" according to InterTrust
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	software and/or hardware for receiving and opening S-software	see 2, above	see 2, above	"first apparatus" could be hardware and software for "secure" processing; "governed item" is e.g. request by principle at "second apparatus"
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	tamper-resistant environment, and S-boxes or S-software	see 2, above	see 2, above	first apparatus is a "protected processing environment" according to InterTrust; "rules" is vague but as used alleged by InterTrust in this litigation would include access controls and capabilities, and data integrity
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	a public or private network	a network	a network	nodes transmit and receive
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	see 2, above	see 2, above	see 2, above	See 2(a)
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right	see 2, above	see 2, above	see 2, above	See 2(a)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
	received as part of a signed license (WMRM SDK, Step9)				
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	see 2, above	see 2, above	see 2, above	See 2(a)(5)
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	see 2, above	see 2, above	see 2, above	See 2(a)(6)
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 2, above	see 2, above	see 2, above	See 2(a)(7)
(b) a second apparatus including:	2nd consumer's computer	see 2, above	see 2, above	see 2, above	any 2d node
(1) user controls,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(2) a communications port,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(3) a processor,	2nd consumer's computer	see 2, above	see 2, above	see 2, above	See 28(b)
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	see 2, above	see 2, above	see 2, above	See 2(a)(4)
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	see 2, above	see 2, above	see 2, above	See 2(a)(5) e.g. the verification info is a "rule" according to InterTrust; it verifies the certificate and decrypts the encrypted portion
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules	see 2, above	see 2, above	see 2, above	See 2(a)(6)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Superdistribution ("Mori/Cox")	Griswold	Cryptolopes; iOpener, iPower	Lampson
to at least in part govern at least one aspect of access to or use of a governed item;	in combination				
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	see 2, above	see 2, above	see 2, above	See 2(a)(7)
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	a "clearinghouse" or permissions and/or rights "issuer"	license server	C: royalty/ license clearing center, or smart card iO: UMS iP: e.g. "VDE"	certificate authority
29. A system as in claim 28,					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	see 28(c)	System of 28(c)	System of 28(c)	System of 28(c)

U.S. PATENT NO. 6,185,683 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
2. A system including:		Reference is made to S. Muftic, Security Mechanisms for Computer Networks (Halstead Press, a div. of John Wiley & Sons, 1984)	See deciphering techniques, methods, systems and procedures described in e.g. Kahn, Denning, Muftic, Davies, PEM, and Computer Security (Time Life 1990).	eference is made to the Hellman references cited in the asserted patents, including USP 4,658,093, "New Directions," and "Multi-user Cryptographic Techniques."	Reference is made to D. Denning, "Secure Personal Computing in an Insecure Network," Comm. of the ACM, vol. 22 No. 8 (August 1979); See also, e.g., D. Denning, Cryptography and Data Security (Addison-Wesley 1982)
(a) a first apparatus including,	Consumer's computer, as shown in WMRM SDK	Any computing device, e.g. a computer associated with receiver B (e.g., a merchant) receiving a cheque.	The above references plainly indicate that a networked and/or stand-alone computer may be used to perform the steps of such techniques, methods and procedures.	player and/or base unit	any user's computer (see, e.g., Figs. 2-5)
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	has user controls	see 2(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a comm port	see 2(a)
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	a processor	see 2(a)
(4) a memory storing:	Consumer's computer, as shown in WMRM SDK	See 2(a)	see 2(a)	and a memory	see 2(a)
(i) a first secure container containing a governed item, the first secure container governed item being at least in part encrypted; the first secure container having been received from a second apparatus;	Secure container (packaged Windows Media file), received by consumer's computer from "Content provider" (WMRM SDK, Step 3), which contains encrypted governed item ("Encrypted content")	Encrypted cheque transmitted by A and stored in a memory location associated with B containing signature, value, date etc.	an at least partly encrypted message or file (e.g., signed and/or sealed using a symmetric or asymmetric method)	program from 2d apparatus (e.g. purchased at store or by phone) that requires authorization to be used	a file F, message X, or "secure" communication, containing any encrypted content
(ii) a first secure container rule at least in part governing an aspect of access to or use of said first secure container governed item, the first secure container rule [sic], the first secure container rule having been received from a third apparatus different from said second apparatus; and	Rights portion of signed license, received by consumer's computer from "License issuer" (WMRM SDK, Step 9)	"rules" (such as validity time, check number, ID etc.) used to "open" and validate the cheque, and/or Secret Key (SKC) provided by the bank C	the deciphering code, tool. algorithm and/or data	any of one or more rights or requirements received from a 3d apparatus, such as signed authenticator and/or base unit or key info	file access rules and/or authorization and/or authentication and/or keys obtained from another apparatus, e.g.detachable S-key device, Alt-P generating software, another computer, or Central Facility
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Windows Media Player and Windows Media Rights Manager	system hardware or software used for e.g. "receiving" and "opening" electronic cheques	deciphering system hardware or software	system hardware or software	software or hardware for receiving and opening files, messages, and/or communications
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container; and	1st and 2nd rules consist of any two valid rules as specified in the Window Media Rights Manager SDK; protected processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	receiver B system uses keys provided by A and C and/or specified value, date, validity time, check no., ID etc. to "open" and validate electronic cheques	any 2nd "rules" used in deciphering the message, such as in the algorithm, data or method used to verify a signature or decrypt or display a file or message	processing has safeguards; see above re e.g. BLP "rules," which Hellman supplements (see '193 chart)	systems can be confined, and/or keys recorded in sealed memory chip or magnetic stripe card
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Any hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Any hardware or software used to receive or transmit electronic cheques	system hardware or software used to receive or transmit files or messages	hardware or software is used for transmission	a public or private network
28. A system including:					
(a) a first apparatus including;	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
(1) user controls,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(2) a communications port,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(3) a processor,	Consumer's computer, as shown in WMRM SDK	See 2(a) above	See 2(a)	See 2(a)	see 2, above
(4) a memory containing a first rule,	Memory is in the consumer's computer, first rule is a right received as part of a signed license (WMRM SDK, Step9)	See 2(a)(4) above	See 2(a)(4)	See 2(a)	see 2, above
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	Consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via Windows Media Player and Windows Media Rights Manager.	See 2(a)(5)	See 2(a)(5)	See 2(a)	see 2, above
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware or software used for applying said first rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager	Hardware or software that uses "rules" such as ID, date, value limits, check no., validity time to access, open and sign cheques; see also 2(a)(6)	See 2(a)(6)	See 2(a)(6)	see 2, above
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Hardware or software used to transmit checks, keys etc. between entities A, B and/or C	See 2(a)(7)	See 2(a)(7)	see 2, above
(b) a second apparatus including:	2nd consumer's computer	Any computer associated with a 2nd receiver B (e.g., a 2nd merchant)	a 2nd computer used for deciphering messages or files	any second user's computer	see 2, above
(1) user controls,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(2) a communications port,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(3) a processor,	2nd consumer's computer	See 28(b) above	See 28(b)	See 28(b)	see 2, above
(4) a memory containing a second rule,	Memory is in 2nd consumer's computer, first rule is a Right received as part of a signed license (WMRM SDK, Step 9)	See 28(a)(4); 2nd "rule" may be ID, date, or signature of A that is unique to a given cheque	See 28(a)(4)	See 2(a)(4)	see 2, above
(5) hardware or software used for receiving and opening secure containers, said secure containers each including the capacity to contain a governed item, a secure container rule being associated	2nd consumer's computer receives Windows Media file (secure container) via communications port (WMRM SDK, Step 3) and applies secure container rule or rules via	See 28(a)(5)	See 28(a)(5)	See 2(a)(5)	see 2, above

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Muftic	deciphering a file or message	Hellman	Denning
with each of said secure containers;	Windows Media Player and Windows Media Rights Manager.				
(6) a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said apparatus, said protected processing environment including hardware or software used for applying said second rule and a secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item;	Processing environment includes Windows Media Rights Manager and Windows processes for protecting operation of Windows Media Rights Manager; processing environment applies multiple rules in combination	See 28(a)(6)	See 28(a)(6)	See 2(a)(6); processing environment may apply multiple rules in "combination" according to InterTrust's usage	see 2, above
(7) hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses; and	Hardware or software employed in transmitting Windows Media files, including for example 2nd consumer's computer's communication port and Windows Media Player (WMRM SDK, Step 3)	Hardware or software used to transmit cheques between entities	system hardware or software for transmitting files or messages	See 2(a)(7)	see 2, above
(c) an electronic intermediary, said intermediary including a user rights authority clearinghouse.	License Issuer	Bank C	any "intermediary" computer with a "clearinghouse" function	authorization and billing unit	a Central Facility
29. A system as in claim 28,					
said user rights authority clearinghouse operatively connected to make rights available to users.	License Issuer, operatively connected to consumer's computer (WMRM SDK, Step 9)	Bank C "operatively connected" to plural merchants	"operatively connected" to more than one computer used to decipher messages	system of 28(c)	see 28(c)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

U.S. PATENT NO. 6,253,193 (invalid as alleged by InterTrust)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
1. A method comprising:								
(a) receiving a digital file including music;	Reference is made to the Windows Media Rights Manager SDK Programming Reference ("WMRM SKD"), attached hereto as Exhibit A. Media Player infringement analysis is set forth herein using the example of a music file downloaded and transferred to a portable audio player. Consumer receives a Windows Media file (WMRM SDK, Step 3)	See references in '683 chart above, e.g., USP 5,634,012; 5,715,403; 5,629,980; and 5,638,443; col:line references below refer to the '012 patent. One kind of digital work received at a first device can be an audio file. See e.g., 8:26 ("Examples of a rendering system may be a computer system, a digital audio system, or a printer") 16:8 (Examples of high value works include movies, digital music) 20:41 (Grammar element "1504 Render-Code" takes values for "Play" for playing, e.g. "digital movies, digital music, playing a video game, running a computer system") 37:51-66 (typically to "play" a work is to use a transducer, e.g. speaker or display) 50:15 (example of pay-per-use application: music demo) "A musician may want to allow extraction of portions of his work but not changing of the tonality"	See reference cited in '683 chart above. "Document" includes audio clips or movies (p1), e.g., MIDI or QuickTime	See Blaze references listed above. Receiving any music file (e.g. MIDI or music program) transferred from one computer or medium to another. As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.	See references in '683 chart above. In e.g. Linn, user (e.g., library or distributor) receives an audio file	See references in '683 chart above, (e.g. US Patent No. 4,658,093). E.g. a customer or store (or other distributor, manufacturer or vendor) receives file including music	See references cited in '683 chart above. Publisher's CUPID Client transmits files and job ticket information to the Origination Server. As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.	Reference is made to the Neuman and Chaum references cited above (see '683 chart). As noted in the accompanying text, and as expressly indicated in e.g. Stefik, Choudhury, Hellman, etc., it was obvious that protections might be applied to digital music.

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
		52:53-58 (definition of Digital Work is "encapsulated digital information such as music")						
(b) storing said digital file in a first secure memory of a first device;	Windows Media file is stored in consumer's computer and all use of it is securely managed by the Secure Content Manager in Windows Media Player.	Digital works are stored in secure repositories, e.g. repository 201 in Fig. 1 8:27 ("A rendering system has the same security features as a repository") 16:7-15 (repositories suitable for holding valuable digital works like bearer bonds & first run movies can have "elaborate measures for ensuring physical integrity and for verifying authorization before use") See col. 16, Table 2 (Repository security levels 0-10)	client or server memory	file stored in a device	object is stored in a form which may not be displayed or printed without the rendering software unless it is extracted from within its envelope and is an authorized copy	stores files "securely," using one or more techniques or combination thereof (e.g., permissions, ACLS, logins, keys and locks, physical security)	Origination Server packages the file content into a Printjob	exchange of music file (e.g. data or audio programming or multimedia) using budgets and other authorization and authentication techniques and capabilities of Neuman and/or Chaum.
(c) storing information associated with said digital file in a secure database stored on said first device, said information including at least one budget control and at least one copy control, said at least one budget control including a budget specifying the number of copies which can be made of said digital file; and	License is stored in the License Store (WMRM SDK, Step 5); license includes Rights which may include AllowTransferToNonSDMI, AllowTransferToSDM.	- info associated with music file can include usage rights, expressed in a URG (usage rights grammar). See list at Fig. 15: Control examples include: Right Code (e.g. Transport code, including right to copy, transfer, loan), Derivative Work Code, & Next-Set of Rights; Budget control examples include Copy Count. See also Fig. 10 (rights portion of designation block of Fig. 7): includes rights code 1050 and status info 1052 7:61 (authorization/digital certificate can itself be a digital work that moves between repositories subject to usage rights)	"documents" may have different levels of security, rendering requirements, granular levels of billing and access, access control, authentication (including Kerberos), persona, anonymous. See '683 ¶ 2(a)(4)(ii)	operation budget and copying information associated with file is stored (e.g., by or for root or other user of certain level or privilege) on device	active and passive protections control copying; authorized use meter and/or "copy counter" can be employed to limit number of copies	Stores associated budget control and/or copy information in secure manner	Scenario A) the Workflow Management Service stores data e.g. for tracking dates and file removal Scenario B) Each Printjob created contains a specified header including copy counters. The budget control is in the header of each Printjob record that is created.	storing associated at least one "budget" and "copy control" for commerce and/or other management or policy

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art
– see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
said at least one copy control controlling the copies made of said digital file;								
(d) determining whether said digital file may be copied and stored on a second device based on at least said copy control;	Windows Media Rights Manager enforces the license restrictions	Usage right(s) (e.g. Transport-Code, Time-Spec determine whether the file can be copied, e.g. to rendering repository 203 in Fig. 2. Repository 201 is coupled to a rendering device to comprise a "rendering system" 7:66-8:3, 8:22 et seq.)	e.g., rights/permissions/ credentials determine whether the file can be copied to 2d device	directory and/or file keys, permissions, rights, and/or privileges determine whether file may be copied to 2nd device	-"write protect" status determines whether can copy - rendering program determines whether to copy and store on an output device, e.g. a video display or printer or audio device	determines whether file may be copied to base unit or player, or played (e.g. to be recorded on another device while playing)	Origination Server governs whether files can be transferred; CUPID clients receive files based on information they receive via their message queues and notification servers	One or more rights, permissions, keys and/or credentials effect "copy control"
(e) if said copy control allows at least a portion of said digital file to be copied and stored on a second device,	Windows Media Rights Manager determines whether the AllowTransferToNonSDMI or AllowTransferToSDMI rights are present	if copy is allowed,	if copy is allowed,	if allowed to copy	if allowed	if allowed,	if allowed	if allowed,
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	a copy is made,	a copy is made,	a copy is made	a copy is made	copy is made,	a copy is made	copy is made,
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output.	and transferred to the memory of the rendering repository; the music file is stored in a repository, either ephemerally or permanently (or it could be stored in the music-equivalent of the "printer repository" of 8:39-46)	and transferred to a memory of 2d device with a speaker and/or video output	file is copied to a 2nd device including a memory and an audio and/or video input (e.g. a PC)	2d device includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output	and transferred to a 2d device which includes a memory and audio and/or video output
(3) storing said digital file in said memory of said second device; and	Music file is transferred to the portable device	file is transferred	file is transferred	storing the file in the 2nd device's memory	"document" is transferred	where it is stored	CUPID Client stores	where it is stored
(4) including playing said	Portable device plays the music	Played, in URG sense and in sense of being rendered (e.g. 20:41)	and played	music played	render on 2d device	and played	and renders	and played

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
music through said audio output.								
2. A method as in claim 1, further comprising:								
(a) at a time substantially contemporaneous with said transferring step, recording in said first device information indicating that said transfer has occurred.	Counter reflecting TransferCount is decremented by Windows Media Rights Manager	e.g. Copy Count or remaining loan is a variable	transfer information recorded	system/host logs transfer event and e.g. CPU time and/or memory	library/distributor records transfer to 2d device (e.g., library may record "loan")	accounting for transfer	Origination Server decrements count for Printjob	transfer accounted for
3. A method as in claim 2, in which:								
(a) said information indicating that said transfer has occurred includes an encumbrance on said budget.	Counter decrement reduces the allowable number of budgeted transfers	Total Copy Count, or total loan ability, are "budget" values that get decremented. See also Table 1 (Digital Work State Information).	encumbering a "budget"	transfer encumbers a "budget"	permitted number of copies decremented	transfer reduces number of allowable transfers	see 2(a)	by an "encumbrance" on the "budget"
4. A method as in claim 3, in which:								
(a) said encumbrance operates to reduce the number of copies of said digital file authorized by said budget.	Counter decrement reduces the allowable number of budgeted transfers	Copying or loaning reduces the number of authorized copies	reducing the number of authorized copies	encumbrance operates to reduce remaining number of copies authorized by user budget	see 3(a)	transfer reduces number of allowable transfers	see 2(a)	transfer can reduce number to be allowed
11. A method comprising:								
(a) receiving a digital file;	onsumer receives a Windows Media file (WMRM SDK, Step 3)	See 1(a)	See 1(a)	Host receives encrypted file	File is a "sealed object"	See 1(a)	See 1(a)	See 1(a)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
(b) storing said digital file in a first secure memory of a first device;	Windows Media file is stored in consumer's computer and all use of it is securely managed by the Secure Content Manager in Windows Media Player.	See 1(b)	See 1(b)	Stores in memory managed by Unix/CFS	storing file in memory of a device	See 1(b)	See 1(b)	See 1(b)
(c) storing information associated with said digital file in a secure database stored on said first device, said information including a first control;	License information is stored in the License Store (WMRM SDK, Step 10), license information includes Rights. License Rights may include AllowTransferToNonSDMI, AllowTransferToSDMI, LicenseCount	See 1(c) E.g., "Certain communications and transactions may be conditioned on a repository being in a particular security class."	rights and levels stored in memory	Information associated with the file is stored in memory (e.g., a CFS directory) by Unix/CFS and includes a first "control" (e.g., a particular permission or right or key)	storing "control" information in memory	usage rights or access controls	Origination Server creates Printjob, uses Workflow Management Service, records requirements, tasks and prerequisites needed in order to process	storing any of numerous positive or negative credentials, rights, or restrictions associated with file
(d) determining whether said digital file may be copied and stored on a second device based on said first control,	WMRM determines whether transfer rights are included in license (WMRM SDK, Step 5)	No copy is stored on 2d repository (or the rendering hardware) if the usage rights and/or security level information and/or access controls don't allow it	copy made or not depending on a "control"	Based on the "control," determines whether file can be copied to 2nd device	control may be used to determine whether file can be copied to 2d device using the rendering software	copy made or not depending on a "control"	Origination Server checks copy controls to determine whether to transfer Printjob to Printshop	copy made or not depending on a "control"
(1) said determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said second device, said determination based at least in part on the features present at the device to which said	Portable Device Service Provider Module identifies the portable device as either SDMI-compliant or non-SDMI-compliant and provides this information to Windows Media Device Manager, which allows the transfer based on whether the device identification matches the License Right.	Usage rights, security level check and/or access control check may fail based on 2d device's identity	checking 2d device	2d device may be identified and transferability determined based on one or more of its features	based at least in part on features of 2d device (e.g., does user have "write" privileges to 2d device; or is the user identification a match; or is the 2d device able to receive data, e.g. using a given protocol)	2d device may be identified and transferability determined based on one or more of its features	Origination Server initiates contact with Notification Server running at Printshop and requests the PSP (Printshop Specification Record) containing information regarding the capabilities of the Printshop	2d device may be identified and transferability determined based on one or more of its features

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
copied file is to be transferred;								
(e) if said first control allows at least a portion of said digital file to be copied and stored on a second device;	If Windows Media Rights Manager determines whether the AllowTransferToNonSDMI or AllowTransferToSDMI rights are present, the following steps are performed:	depending on the usage rights/security level/ACL check	depending on the check results	If the control allows the copying	if copy is allowed	if copy is allowed	If the PSP specifications match those required by the Printjob,	if copy is allowed
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	a copy may be made	copy may be made	The file is copied	copy may be made	copy may be made	CUPID Client is notified that the Printjob is available to be received	copy may be made
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output	and transferred to a 2d repository with video and/or audio output	and transferred to 2d device with video and/or audio output	To a device with video and/or audio output (e.g., a PC)	and transferred to 2d device with video and/or audio output	and transferred to 2d device with video and/or audio output	file transferred	and transferred to 2d device
(3) storing said digital file in said memory of said second device; and	Music file is stored in the portable device	stored there	stored there	Stored in memory	stored there	stored there	stored	stored there
(4) rendering said digital file through said output.	Portable device plays the music	and rendered through audio and/or video output	and rendered	And rendered	and rendered	and rendered	and rendered	and rendered
15. A method comprising:								
(a) receiving a digital file;	onsumer receives a Windows Media file (WMRM SDK, Step 3)	A digital work is received	User receives a file	An encrypted file is received at e,g, host or user divice	File received	Vendor or base unit receives file	Origination Server receives digital file from CUPID Publisher Client	File received
(b) an authentication step comprising:							Publisher logs in to authenticate identity	
(1) accessing at	License includes identity of	See Table 2. Various authentication	user or "device"	"device" or user	user or "device"	check for base unit;	Publisher assigns an	user or "device"

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
least one identifier associated with a first device or with a user of said first device; and	user's Windows Media Player	"identifiers" can be accessed. "A repository will have associated with it a repository identifier. Typically, the repository identifier would be a unique number assigned to the repository at the time of manufacture. ... As a prerequisite to operation, a repository will require possession of an identification certificate. Identification certificates are encrypted to prevent forgery and are issued by a Master repository." - Works can be signed - Passwords can be associated with users or devices - Physical security comprises known authentication steps	"identifier" accessed according to InterTrust	"identifier" accessed, e.g., login or password or signature or address or number	"identifier" accessed according to InterTrust	or check e.g. password or ACL or key	Order Name and authorization codes for documents	"identifier" accessed according to InterTrust
(2) determining whether said identifier is associated with a device and/or user authorized to store said digital file;	Music file cannot be used unless identifier indicated in License matches user's Windows Media Player identifier	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	authentication succeeds or fails	Checks login, or authorization codes against valid system users via standard Unix login measures or through secure PKI authentication techniques	authentication succeeds or fails
(c) storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized.	Music file will not be processed through Windows Media Player, including protected rendering buffers, unless the identifiers match	Digital work is stored in repository only if authentication succeeds	file is "processed" only if authentication succeeds	"storing" occurs if authorized	file is "processed" only if authentication succeeds	file is "processed" only if authentication succeeds	If authorized as a valid document publisher, the Origination Server allows the files to be stored on the Origination Server; see 1(a)	file is "processed" only if authentication succeeds
(d) storing	License includes Rights and is	associated usage right(s) or security	license rights	see 11(c)	attributes are stored	rights include limits	See 11(c)	See 11(c)

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
information associated with said digital file in a secure database stored on said first device, said information including at least one control;	stored in the License Store, Rights may include AllowTransferToNonSDMI, AllowTransferToSDMI, LicenseCount	level information is stored on 1st device; see also 11(c)	include limits on transfer; see also 11(c)		with associated object; see also 11(c)	on transfer; see also 11(c)		
(e) determining whether said digital file may be copied and stored on a second device based on said at least one control;	Windows Media Rights Manager enforces the license restrictions	System enforces usage rights and levels	See 11(d)	See 11(d)	rendering software enforces restrictions	See 11(d)	See 11(d)	See 11(d)
(f) if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	If appropriate rights are present, the following steps are performed:	if copying and storing a portion of file is allowed	See 11(e)	See 11(e)	if copying and storing a portion of file is allowed	See 11(e)	See 11(e)	See 11(e)
(1) copying at least a portion of said digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	The digital work is copied	See 11(e)(1)	copies if permitted	at least a portion is copied	file or portion copied	See 11(e)(1)	See 11(e)(1)
(2) transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;	Portable device necessarily includes at least a memory and audio output	and transferred to 2d repository	See 11(e)(2)	2nd device includes memory and audio and/or video output (e.g., PC has monitor and/or speaker)	and transferred to 2d device	and transferred	See 11(e)(2)	See 11(e)(2)
(3) storing said digital file in said memory of said second device; and	Music file is stored in the portable device	where it's stored	See 11(e)(3)	file is stored	stored there	stored	See 11(e)(3)	See 11(e)(3)
(4) rendering said digital file	Portable device plays the music	and rendered	See 11(e)(4)	and rendered	and rendered	and rendered (e.g., at base unit, or at	See 11(e)(4)	See 11(e)(4)

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
through said output.						player or other 2d device)		
19. A method comprising:								
(a) receiving a digital file at a first device;	WMRM SDK, Step 3.	A digital work is received at a first repository	file received	Receive file at device (e.g., download or floppy at "device" on Unix/CFS network, e.g. earlier in or in earlier session).	user receives file	file received	Origination Server	file received
(b) establishing communication between said first device and a clearinghouse located at a location remote from said first device;	WMRM SDK, Step 6.	any 2nd repository, including but not limited to a billing repository, can act as a "clearinghouse" communicating w/ a physically remote 1st repository	communication established with repository acting as "clearinghouse" (see '683 ¶ 28(c))	establish communication with any "clearinghouse" device in Unix/CFS network	user communicates with any "clearinghouse" device, e.g. library	communication with any "clearinghouse" device, e.g. vendor or authorization unit	Agent running at the Origination Server communicates with a "clearinghouse"	"clearinghouse" as alleged by InterTrust is met by any certificate server or other device capable of transacting with multiple users
(c) said first device obtaining authorization information including a key from said clearinghouse;	WMRM SDK, Step 9.	"clearinghouse" repository provides authorization information "including a key"	"clearinghouse" supplies authorization information "including a key"	Device obtains key from system	user obtains authorization info	"clearinghouse" supplies authorization information "including a key"	Agent running at Origination Server checks to see if included subdocument files are authorized for use by the publisher, and receives authorization notification from clearinghouse	"clearinghouse" supplies authorization information "including a key"
(d) said first device using said authorization information to gain access to or make at least one use of said first digital file, including using said key to decrypt at least a portion	WMRM SDK, Step 11.	Authorization information used for access or use (& key use to decrypt digital work, which may be usage rights)	authorization information used for access or use	Device uses key to decrypt at least a portion of the file	authorization information used for access (e.g., uses file's public key to decrypt its signature)	authorization info used for access or use	E.g. stock image files may be partly encrypted; access to images must be granted through clearinghouse servers and payment servers, allowing subdocuments to be transmitted to the	key used to decrypt

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
of said first digital file: and							Origination Server, decrypted and ultimately included into final Printjob by Document Assembly Service	
(e) receiving a first control from said clearinghouse at said first device;	WMRM SDK, Steps 8-9.	one or more "controls" is received from "clearinghouse" repository	one or more "controls" received from "clearinghouse"	Receives file permissions or key	a "control" comes with the file	a first "control" received	Right to reproduce authorization is received by Origination Server	a first "control" received
(f) storing said first digital file in a memory of said first device;	WMRM SDK, Step 3.	Digital work stored in a 1st device's memory	File stored	File stored	File stored	File stored	File stored, E.g. Workflow Management Service communicates with Document Assembly Service that creates printable materials by assembling subdocuments referenced during publishing step	File stored
(g) using said first control to determine whether said first digital file may be copied and stored on a second device;	At least the following WMRMRights Object properties meet this limitation: AllowTransferToNonSDMI, AllowTransferToSDMI TransferCount	"control" determines whether file can be copied to 2d device	"control" determines whether file can be copied to 2d device	Uses permissions or key to determine whether can copy to another device	"control" determines whether file can be copied to 2d device	and used to determine whether file maybe copied and stored on 2d device	Authorization is checked prior to including files in Printjob	and used to determine whether file maybe copied and stored on 2d device
(h) if said first control allows at least a portion of said first digital file to be copied and stored on a second device;	This and all subsequent claim steps occur when the condition specified in the WMRMRights Object property is met	if the copying is allowed	if the copying is allowed	If permission key allows or signature works	if the copying is allowed	if copy is allowed	If Authorization is granted then the file can be copied	if copy is allowed
(i) copying at least a portion of said first digital file;	Transfer to the SDMI or non-SDMI portable device, if allowed by Windows Media Rights Manager	copying occurs	copy made	The file is copied	copy made	a copy may be made	CUPID Client copies	a copy maybe made
(j) transferring at	Portable device necessarily	the work is transferred	transferred	Transferred to a 2nd	transferred	transferred	transfers	transferred

Charts demonstrating the invalidity of '683 & '193 asserted claims as alleged by InterTrust in view of prior art – see accompanying text for further explanation of invalidity, including obviousness and § 112

CLAIM LANGUAGE (InterTrust's version)	INTERTRUST'S PLR 3-1 STATEMENT	Stefik	Choudhury, Maxemchuck et al.	Blaze	CNI/IMA 94	Hellman	CUPID	Neuman and/or Chaum
least a portion of said first digital file to a second device including a memory and an audio and/or video output;	includes at least a memory and audio output			device with memory and audio and/or video output				
(k) storing said first digital file portion in said memory of said second device; and	Music file is stored in the portable device	stored in the 2d device	stored	Stored in 2nd device memory	stored	stored	stores	stored
(l) rendering said first digital file portion through said output.	Portable device plays the music	and rendered through audio and/or video output	and rendered	And rendered.	and rendered	and rendered	and renders	and rendered

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

AND COUNTER ACTION.

No. C 01-1640 SBA

Consolidated with C 02-0647 SBA

ORDER GRANTING DEFENDANT MICROSOFT CORPORATION'S RENEWED MOTION FOR PARTIAL SUMMARY JUDGMENT OF NONINFRINGEMENT OF THE GRISWOLD PATENT

[Docket No. 510]; directed to serve this ... other parties in this actions.

In view of plaintiff's statement of non-opposition to defendant's Renewed Motion for Partial Summary Judgment of Noninfringement of the Griswold Patent,

IT IS HEREBY ORDERED THAT defendant's Renewed Motion for Partial Summary Judgment of Noninfringement of the Griswold Patent is GRANTED.

IT IS FURTHER ORDERED THAT the Case Management Conference scheduled for May 7, 2002 is CONTINUED to May 23, 2002 at 3:00 p.m. Plaintiff's counsel is to set up the telephonic conference call with all the parties on the line and call chambers at (510) 637-3559 at the time designated above. NO PARTY SHALL CONTACT CHAMBERS DIRECTLY WITHOUT PRIOR AUTHORIZATION OF THE COURT. Since the parties filed a Joint Case Management Statement on April 26, 2002, the parties need not file a new Statement unless changed circumstances warrant the filing of an updated statement. Any updated statement shall be filed at least five (5) days in advance of the new CMC date.

IT IS SO ORDERED.

Dated: May 3, 2002

SAUNDRA BROWN ARMSTRONG
United States District Judge

PATENT
Customer Number 22,852
Attorney Docket No. 07451.0001.10
InterTrust Ref. No.: IT-5.0.2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Karl L. GINTER et al.	)	Group Art Unit: 2132
	)	
Serial No.: 09/328,668	)	Examiner: G. Barron, Jr.
	)	
Filed: June 9, 1999	)	
	)	
For: SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION	)	

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

NOTICE REGARDING RELATED LITIGATION

Applicants hereby notify the U.S. Patent and Trademark Office that several patents assigned to InterTrust Technologies Corporation ("InterTrust") are involved in litigation. The present application, Serial No. 09/328,668, is a continuation of U.S. Patent No. 5,982,891, which is one of the patents at issue in the litigation, and shares a common parent with U.S. Patent Nos. 6,389,402 B1; 6,253,193 B1; 6,185,683 B1; 5,949,876; 5,917,912; 5,915,019; and 5,892,900, which are also at issue in the litigation.

STATUS OF RELATED LITIGATION

The status of the litigation is as follows. On April 26, 2001, InterTrust filed a Complaint alleging that Microsoft Corporation ("Microsoft") was infringing U.S. Patent No. 6,185,683 B1,

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On May 14, 2002, I served:

ORDER GRANTING DEFENDANT MICROSOFT CORPORATION'S RENEWED MOTION FOR PARTIAL SUMMARY JUDGMENT OF NONINFRINGEMENT OF THE GRISWOLD PATENT

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page** at **mhp@kvn.com, Christopher P. Isaac** at **chris.isaac@finnegan.com, Stephen E. Taylor** at **staylor@tcolaw.com** and **James E. Geringer** at **james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: jwk@kvn.com
Email: mhp@kvn.com

Attorneys for Plaintiff INTERTRUST TECHNOLOGIES CORPORATION

Stephen E. Taylor, Esq.
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408
Email: staylor@tcolaw.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

Christopher P. Isaac, Esq.
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I. Street, N.W.
Washington, DC 20005-3314
Tel. No. 202-408-4000
Fax No. 202-408-4400
Email: chris.isaac@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: john.vandenberg@klarquist.com
Email: james.geringer@klarquist.com

Attorneys for Defendant and Counterclaimant, MICROSOFT CORPORATION

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on May 14, 2002 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

ANNA FREDDIE